American Water Works Association

Dedicated to the World's Most Important Resource®

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

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 AWIA 2018 §2013 compliance. 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.

CONTENTS

ACKNOWLEDGEMENTS

This project was funded by the American Water Works Association (AWWA), utilizing Water Industry Technical Action Fund (WITAF), WITAF Project #039, and managed by Kevin M. Morley.

Project Advisory Committee

- Norm Anderson, Carollo Engineers
- John Brosnan, Santa Clara Valley Water District
- Don Dickinson, Phoenix Contact
- Patrick Norton, Tampa Bay Water
- Robert Raffaele, American Water

Project Contractors

- Andrew Ohrt, West Yost Associates
- Dan Groves, West Yost Associates
- Jeff Pelz, West Yost Associates
- Joel Cox, West Yost Associates
- Murphy Altunel, West Yost Associates
- Bailey Bartolucci, West Yost Associates
- Judith H. Germano, GermanoLaw LLC
- Gwen M. Schoenfeld, GermanoLaw LLC
- Gemma Kite, Horsley Witten Group, Inc.
- Tom Noble, Horsley Witten Group, Inc.
- Will Keefer, Horsley Witten Group, Inc.

Subject Matter Expert Panel

- Danielle Anderson, City of Minneapolis Water Treatment and Distribution Services Division
- Will Bianchini, Onondaga County Water Authority
- Andy Bochman, Idaho National Laboratory
- Jacques Brados, Black and Veatch
- Geoffrey Brown, Alameda County Water District
- Bernie Bullert, SL-Serco
- Travis Cochrane, City of Corpus Christi
- Jeff Cooley, City of Vacaville Public Utilities
- Steve Crumley, City of Minneapolis Water Treatment and Distribution Services Division
- Charley Cunningham, City of Sacramento Department of Utilities
- Bob Daly, EMA Inc.
- Jon Eaton, City of Eagan Public Utilities
- Bill Fisher, National Institute of Standards and Technology
- Jamie Foreman, City of Carmel Public Works
- Glen Goins, The Automation Group
- Andrew Hildick-Smith, Massachusetts Water Resource Authority
- Daniel Honore, Village of Pleasant Prairie Utility Department
- Dr. Connie Justice, Indiana University Purdue University Indianapolis
- Marlene Ladendorff, Schneider Electric
- Michael Lewis, City of Albany Public Works
- Jim Livermore, CDM Smith
- Mike Malone, Eastern Municipal Water District
- Blas Moreno, Prince William County Service Authority
- Ariz Naqvi, Alameda County Water District
- Debbie Newberry, United States Environmental Protection Agency
- Janine Nielsen, Rockwell Automation, Inc.
- Kevin Owens, Control Cyber Inc.
- Cayce Parrish, United States Environmental Protection Agency
- David Paul, AquaEngineers
- Chuck Redding, City of Sacramento Department of Utilities
- Nelson Sims, DC Water and Sewer Authority
- Chris Walcutt, Black and Veatch
- Jennifer Lyn Walker, WaterISAC
- Linda Warren, Launch! Consulting

Acronym and Abbreviation Table	
Acronym /Abbreviation	**Description**
ANSI	American National Standards Institute
AWIA 2018	America's Water Infrastructure Act of 2018
AWWA	American Water Works Association
CCE	Consequence-Centered Engineering
CFR	Code of Federal Regulations
CIA	Confidentiality Integrity and Availability
CIA	Confidentiality, Integrity, and Availability
CIE	Cyber-Informed Engineering
CIR	Committed Information Rate
CISSP	Certified Information Systems Security Professional
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
PCI	Payment Card Industry
PCS	Process Control Systems
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
SME	Subject Matter Experts
SSN	Single Sign On
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WITAF	Water Industry Technical Action Fund

EXECUTIVE SUMMARY

Within the last several decades, cybersecurity threats, including such things as cyber-terrorism and ransomware attacks, have grown from the esoteric practice of a few specialists to a problem of general concern. Critical infrastructure systems serving the people of the United States have been found to be particularly vulnerable to such attacks. As noted in the 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 the general threat to critical infrastructure, a wide array of standards and guidelines are available to assist organizations with implementing security controls to mitigate the risk from cyber-attacks. The scope of these documents is large, and the security controls in the standards often require significant planning and years of implementation.

In February 2013, the American Water Works Association (AWWA) Water Utility Council initiated a project (WITAF #503) to address the absence of practical, step-by-step guidance for protecting water sector process control systems (PCS)[2] from cyber-attacks. This action was timely as it corresponded with the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as called for in Executive Order 13636 - Improving Critical Infrastructure Cybersecurity.[3] The NIST Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

This AWWA Water Sector Cybersecurity Risk Management Guidance (AWWA Guidance) and associated AWWA Cybersecurity Assessment Tool (AWWA Assessment Tool), collectively referred to as AWWA Guidance and Assessment Tool, is a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council. The original goal of this AWWA guidance was to provide water sector utility owners/operators with a consistent and repeatable assessment tool and recommended course of action to reduce vulnerabilities to cyber-attacks as recommended in ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636. The guidance is also expected to communicate a "call to action" for utility executives acknowledging the significance of securing PCS and enterprise systems (e.g. information technology) given their role in supporting water utility operations.

This AWWA Guidance and Assessment Tool update was developed to assist community water systems (i.e. utility) in complying with section 2013 of America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270).[4] AWIA requires all community water systems serving populations of 3,300 or more to conduct and certify completion of an assessment of the risks to, and resilience of their systems, including an emergency response plan. The new 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;

---

[1] American Water Works Association, *Cybersecurity Risk and Responsibility in the Water Sector*, 2018.

[2] The term process control system (PCS) is preferred over industrial control system (ICS) to avoid confusion with incident command system (ICS) common in national emergency response planning.

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

[4] The text of AWIA §2013 is included in Appendix A.

- 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).

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

A panel of subject matter experts was consulted to identify the most pressing cybersecurity issues facing water utilities today. In response to these issues, a recommended grouping of cybersecurity practices was developed. This grouping identifies cybersecurity practice areas considered to be the most critical for managing cyber risk 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.

These recommended practices are defined by a set of 99 cybersecurity controls that are organized in a manner to facilitate implementation based on actionable tasks. The outputs of the AWWA Assessment Tool are designed to present these controls to users in a concise, straightforward manner, facilitate documentation and support future compliance actions and improvement.

The AWWA Assessment Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user provides information about the manner in which their PCS and enterprise systems are used. Based on these practices, use cases are selected to recommend controls. For each recommended control, specific references to existing cybersecurity standards are also provided.

The AWWA Assessment Tool emphasizes actionable recommendations with the highest priority assigned to those that are expected to provide the greatest impact in the short term. It should be noted, however, that the tool does not assess the extent to which a utility has implemented any of the recommended controls. This is the responsibility of the utility. To facilitate this, additional tool outputs were added and are discussed in the following sections.

This resource is a living document, and further revisions and enhancements will be made based on the quickly evolving cyber-threat landscape and user feedback.

Use of this Guidance to Support AWIA §2013 Compliance

As noted above, one objective of the AWWA Cybersecurity Guidance and Assessment Tool is to support utilities with AWIA §2013 compliance actions. Additional guidance is provided in subsequent sections of this document.

Utility staff responsible for AWIA §2013 compliance may not be cybersecurity technologists or responsible for the secure and reliable operation of the PCS and/or enterprise systems. Therefore, it is recommended that a utility convene internal and external support staff, including, but not limited to:

- Utility compliance staff responsible for AWIA §2013 compliance.

- Utility staff responsible for and knowledgeable of the design, operation, and maintenance of the utility's PCS and enterprise systems (information technology).
- Utility leadership responsible for overall operation of the utility (utility staff with the authority to accept risks should be present).
- External support staff including cybersecurity vendors, engineering firms, etc., if needed.

This approach will improve the quality and timeliness of data collection. In addition, it is expected to reduce the overall time required to complete compliance actions while also improving the cybersecurity posture[5] of the organization.

Cybersecurity Guidance and Tool Output Information Security

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

- If your utility 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 your jurisdiction.
- If your utility does not have a data classification system in place:
    - Store this data in a secure location.
    - Restrict access to this information as much as possible. For example: do not email this document.

RECOMMENDED CYBERSECURITY PRACTICES

Overview

These practices are comprised of recommendations to improve the cybersecurity posture of water and wastewater utilities. They are actionable recommendations designed to produce maximum improvement in the short term and provide a foundation for longer term implementation of a comprehensive cybersecurity risk management strategy.

The terminology used within this section and other standards is fundamentally technical. AWWA strived to make the guidance and user experience as "plain English" as possible. However, some additional insight into the networking and network component terminology may be helpful to the reader. It is recommended that the reader refer to Appendix B: Network Architecture Reference Diagram and Definitions.

Practice Categories

The practice categories were chosen by Subject Matter Experts (SME) teams during a Definition Workshop. Each team identified important areas of cybersecurity to be addressed and policies, activities, and systems that should be implemented. The recommendations from the SMEs 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 practives 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

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

recommended controls into these practice areas. The following is a description of each practice category.

Governance and Risk Management

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

Cyber supply chain risk management is an important component in the design, operation, and maintenance of PCS and 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.

Although this category of recommendations represents an essential part of an organization's security posture, the related cybersecurity controls have been assigned a slightly lower priority in order to emphasize actionable recommendations that can have significant short-term effects.

Business Continuity and Disaster Recovery

This category is concerned with ensuring that the control system continues running even when faults occur and with rapid recovery after a service disruption.

Business Continuity Planning is a structured method for an organization 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.

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 whitelisting, which restricts the applications that are permitted to run on servers and workstations throughout the enterprise.

Access Control

This category is concerned with ensuring that only authorized personnel are permitted to access computing resources within the organization; it pertains to best practices for restricting access to computing resources and information to authorized users. For example, Single Sign On (SSN) is an access control mechanism that requires users to sign on only once; the SSN system can then use those credentials to control access to a variety of applications. However, care should be taken to ensure that different passwords are used to access PCS and enterprise systems.

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. Utilities 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.

Encryption

This category is concerned with ensuring that only appropriate encryption schemes are used within an organization'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.

Data Security

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

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 PCS network security, particularly network topology requirements within the vicinity of PCS systems and PLC controls. Another area addressed in this category is network management, including port level security.

Physical Security of PCS Equipment

Physical security is a basic requirement for all PCS 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.

Service Level Agreements (SLA)

This category is concerned with the definition and management of contracts that specify services requirements to the organization. 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 organization.

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 PCS network systems typically focus on quality of service (QoS) rather than bandwidth. PCS 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.

Operations Security (OPSEC)

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

Education

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

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.

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 organization. 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 organization. Personnel security also applies to external contractors and service personnel, with the objective to ensure appropriate, lower privileged access to facilities.

Cyber-Informed Engineering

Cyber-Informed Engineering (CIE)[6,7] and the associated Consequence-Centered, Cyber-Informed Engineering (CCE)[8] are methodologies recently 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 risk. These approaches recognize that, while extremely important, a cyber-hygiene centered approach cannot address the rapidly evolving cyber threats that all critical infrastructure owners and operators face. Therefore, utilities need to take additional measures to ensure that their systems are cyber-resilient.

---

[6]Anderson, Robert S., Benjamin, Jacob, Wright, Virginia L., Quinones, Luis, and Paz, Jonathan. Cyber-Informed Engineering. United States: N. p., 2017. Web. https://doi.org/10.2172/1369373

[7]Wright, Virginia. Cyber-Informed Engineering. Fermilab Colloquium. September 21, 2016. https://vms.fnal.gov/asset/detail?recid=1944478&recid=1944478

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

CYBERSECURITY TOOL USER GUIDANCE

Overview

The Assessment Tool uses several steps to collect user input on the utility's current cybersecurity posture and provides recommended controls to facilitate AWIA §2013 compliance and cybersecurity improvements. PLEASE NOTE: AWWA DOES NOT COLLECT ANY DATA ENTERED INTO THE TOOL OR ABOUT USERS OF THE TOOL. Rather, this guidance and the Assessment Tool provide the user with recommended controls based on how the utility describes the application of certain technologies and practices in their day-to-day operations. No security sensitive information is required or shared by the user. The process flow of the tool is segmented to address the two primary phases of AWIA §2013, 1) Risk and Resilience Assessment (RRA; dark blue box) and 2) Emergency Response Planning (ERP; green box), is illustrated in Figure 1.

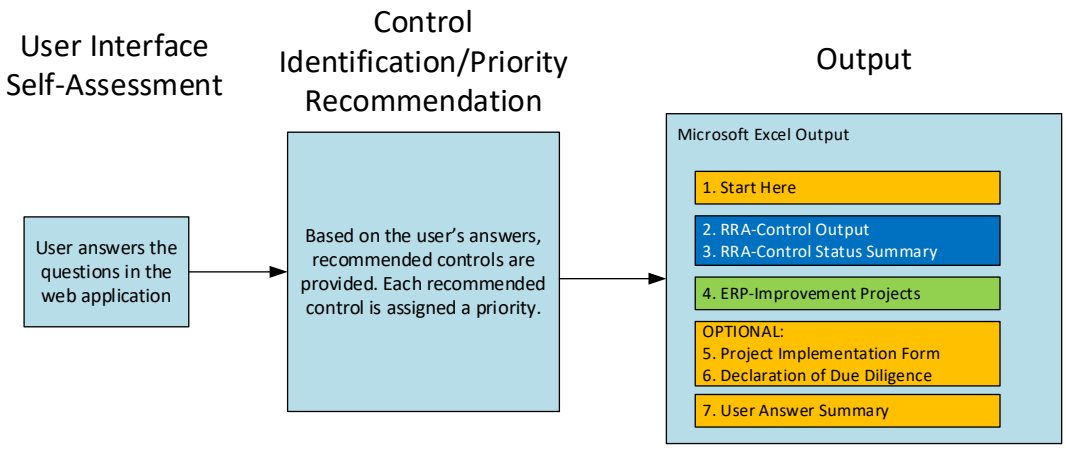

Figure 1. AWWA Cybersecurity Tool Process

The following sections provide additional detail on the individual inputs, processing steps, and outputs of the AWWA Assessment Tool.

User Interface

First, the user answers questions on the policies, procedures and use of their PCS and enterprise systems in the web application. The AWWA Assessment Tool automatically maps the utility's PCS and enterprise system configuration and practices to the recommended control. The questions designed to capture the utility's PCS and enterprise system configuration and practices are included in a worksheet format in Appendix C of this guidance.

Use-Cases

A use-case is an elemental pattern of behavior as described by the user of a system; the use-cases in this document are basic descriptions of important processes from the user's perspective. Based on the use-cases selected, the tool provides recommended cybersecurity controls. Appendix D includes a table

summarizing the use-cases included in the tool. These are no longer visible to the user, but were retained to maintain consistent mapping of controls.

Cybersecurity Controls

A security control is a measure to support effective cyber defense. Most of the controls in this document are measures designed to reduce risk; they were developed from many industry standards which were correlated, integrated, and enhanced. For example, multiple similar controls were merged into a single, more comprehensive control. Some controls are complex and might resemble an administrative program, a computer system, or an engineering design methodology. Many cybersecurity service vendors provide computer systems to implement controls of greater complexity (e.g., network monitoring tools). Appendix E provides a list of the cybersecurity controls developed for this document and a table mapping the controls presented in Appendix E to the controls presented in the NIST Cybersecurity Framework v1.1 is included as Appendix F.

Each control was assigned a priority level based on its criticality and potential impact to the security of the utility. The recommended controls are categorized into priorities 1, 2, 3, and 4, with priority 1 being the highest. For each recommended control, a reference is provided to a set of existing cybersecurity standards. Priority levels are adapted from SANS[9] and are defined as follows:

- **Priority 1 Controls** – These controls represent the minimum level of acceptable security for PCS and enterprise systems. If not already in place, these controls should be implemented immediately. In some cases, they could be considered q*uick wins* that provide solid risk reduction without major procedural, architectural, or technical changes to an environment. Alternatively, a control may provide substantial and immediate risk reduction against common attacks. Generally, these will be cyber-hygiene measures. Utilities with many Priority 1 controls to implement will likely be reactive to any cyber-attack.

- **Priority 2 Controls** – These controls build on those in the Priority 1 category. Despite being Priority 2, these controls have the potential to provide a significant and immediate increase in the security of the organization. Generally, these will be more sophisticated cyber-hygiene measures to improve the process, architecture, and technical capabilities of the utility. These improvements include capabilities such as monitoring of networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

- **Priority 3 Controls** – These controls improve information security configuration and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage. These controls lay the foundation for sustained implementation of a managed security system. These controls include

[9] SANS. CIS Critical Security Controls: Guidelines. https://www.sans.org/critical-security-controls/guidelines. Last accessed May 1, 2019.

more sophisticated longer-term approaches to managing cyber-risk including CIE and cyber supply chain risk management.

- **Priority 4 Controls** – These controls are more complex and provide proactive protection against more sophisticated attacks. These include new technologies, policies, and methods that provide maximum security but are more complex and potentially more expensive than commoditized security solutions.

Maturity is a concept that is widely used in other sectors. Generally, the maturity of an organization's cybersecurity posture is the extent to which a utility has implemented the recommended controls. It is also reflective of a utility moving from a *reactive* to a *proactive* cybersecurity posture. Adapted from SANS,[10] Figure 2 illustrates notional levels of maturity.

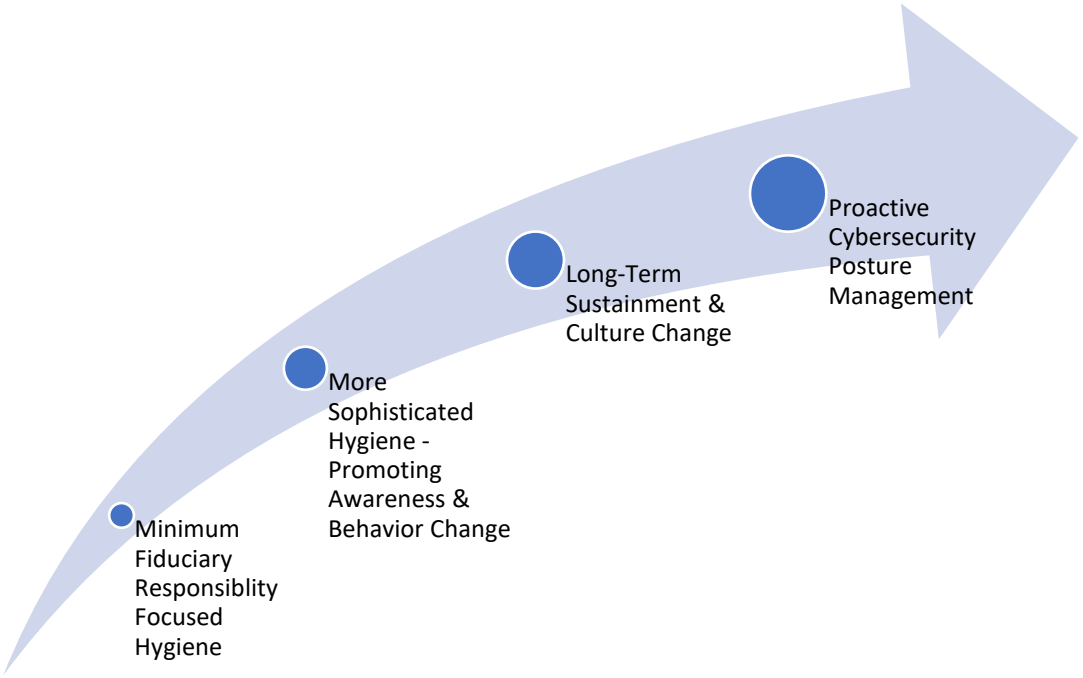

Figure 2. Conceptual Cybersecurity Maturity Levels of an Organization

The maturity levels in Figure 2 are comparable to Tiers 1 through 4 in the NIST Cybersecurity Framework. The Tiers range from Tier 1 – Partial to Tier 4 - Adaptive. The Tiers describe the degree to which a utility's cybersecurity risk management practices exhibit the characteristics defined in the NIST Cybersecurity Framework.[11]

Using this guidance and the Assessment Tool, utilities should assess the controls in place and their associated implementation status (i.e. maturity) on a recurring basis relative to the current and anticipated needs of the organization, the current cybersecurity posture of the organization, and the

[10] SANS.org. https://www.sans.org/sites/default/files/10_24%20Blog%203%20Commandments.png. Last accessed May 1, 2019.

[11] NIST Cybersecurity Framework. An Introduction to the Components of the Framework. https://www.nist.gov/cyberframework/online-learning/components-framework. Last accessed May 28, 2019.

threat landscape. Broadly, the objective should be to continuously move from the minimum controls in place for fiduciary responsibility and a reactive posture to a proactive posture.

Recommended Cybersecurity Practices and Improvement Projects

Each Practice Category identified in has numerous associated recommended controls and potential improvement projects. Some additional details on potential improvement projects are provided below:

1. **Governance and Risk Management**
    a. Develop a formal, written Cybersecurity Policy that addresses the specific operational needs of PCS and enterprise systems.
    b. Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans.
    c. Perform a vulnerability assessment (e.g. CSET or physical assessment) on a regular basis.
    d. To aid in developing contingency plans, maintain current network asset inventory, baseline, "gold disk," including:
        i. Applications
        ii. Data
        iii. Servers
        iv. Workstations/HMI
        v. Field devices (e.g. PLCs)
        vi. Communications and network equipment
    e. Develop and enforce hardware and software standards in order to limit number of system components
    f. Develop standard specifications language that defines cybersecurity standards for inclusion in all procurement packages for PCS and enterprise systems

2. **Business Continuity and Disaster Recovery**
    a. Develop resilience plans including: Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan. These plans should include:
        i. 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.
        ii. Manual overrides to allow temporary manual operations of key processes during an outage or a cyber-attack.
        iii. Strategies for system redundancy (or offline standby) to ensure key system components can be restored within acceptable timeframes.
    b. Ensure that corporate Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan includes procedures and contact list for PCS and enterprise systems.
    c. Conduct exercises to test and revise plans and build organizational response capabilities.

d. Implement change management program for PLC software; maintain fully commented backups for all PLC programs and test restore process on a periodic basis.
e. Implement change management program for enterprise systems with routine backups and restoration exercises.
f. Test backup and recovery plans regularly.

3. Server and Workstation Hardening

a. Implement whitelisting (allows only specified applications to execute on each specific computer).
b. Maintain support contracts with HMI software vendor and implement antivirus, anti-malware, and operating system patches in accordance with vendor's direction.
c. Implement security patch management program with periodic vulnerability scanning.
d. Implement change management program for applications and infrastructure (routers, etc.)
e. Harden critical servers and workstations.
f. Remove local administrator rights, delete/disable default accounts (OS and application).
g. Rename Administrator account.
h. Disable USB, DVD, and other external media ports.
i. Disable auto-scan of removable media.

4. Access Control

a. Secure PCS and enterprise system access.
    i. Physical access to facilities and equipment.
    ii. Application access to key software functions.
    iii. External access should be controlled. Address requirements for:
        1. File exchange into or out of a network. Include system and software updates.
        2. Data exchange between PCS and enterprise systems such as email (alarms), historical databases, CMMS, LIMS, etc.
        3. Establish off-line or isolated system for testing and patch management, including applications and device programs.
        4. Identify what is required for remote access. Restrict remote access to lowest level of privilege required.
    iv. Vendor, contractor system access on plant (incl. package systems). Vendor or contractor access to system should be manually initiated.
    v. Equipment (e.g. network equipment, field devices) access
b. Secure remote access
    i. Use VPN technologies to protect information in transit.
    ii. Require multifactor authentication (e.g. tokens) for remote access to sensitive functions.
    iii. Limit access to only the minimal level required (e.g. view-only web page).

c. Implement multi-factor authentication for all workstations.
d. Laptops that are used to control PCS or program field devices should be "dedicated for PCS use only" and ports to Internet disabled. All non-essential software should be removed.

5. Application Security

a. Require each PCS or enterprise system user to utilize unique credentials (usernames and passwords) which provide only the required level of access needed to perform their job. Establish policy for strength of password and periodic renewal. Implement automatic lock out after adjustable number of failed log-in attempts.
b. Provide separate accounts for administrator and user functions. Do not allow users to operate with administrator rights unless they are actually administering the system.
c. Provide separate credentials for PCS access compared to enterprise system access. Require different passwords between systems.
d. Implement audit controls such as logging and monitoring of system access and modification.
e. Aggregate system logs and conduct frequent review of network, application and systems events.

6. Encryption

a. Implement device and/or storage encryption where theft or loss of a device is a possibility:
    i. Smartphones, tablets containing sensitive system information.
    ii. Laptops containing programs or other sensitive information.
    iii. Equipment (e.g. administrator passwords).
    iv. Removable media (e.g. tape, disk, USB removable storage).
b. Implement communications encryption:
    i. Wireless communications should be encrypted where possible, regardless of type or range.
    ii. Wired communications over shared infrastructure (e.g. leased, shared) should be encrypted using VPN technologies to protect sensitive information in transit.
c. Implement "best available" encryption.
    i. Use strongest available encryption on existing equipment.
    ii. Identify encryption requirements in specifications for new equipment.
d. Implement encryption of confidential data in on-line repositories.

7. Data Security

a. Implement appropriate measures to accept, process, store, and/or transmit customer billing information. The Payment Card Industry (PCI) priorities include:
    i. Remove sensitive authentication data and limit data retention.
    ii. Protect systems and networks, and be prepared to respond to a system breach.
    iii. Secure payment card applications.
    iv. Monitor and control access to your systems.

v. Protect stored cardholder data.
vi. Finalize remaining compliance efforts, and ensure all controls are in place.

b. Implement controls to protect Personally Identifiable Information (PII)
    i. Understand how PII is defined based on local, state, and federal statutes
    ii. Develop a privacy policy.
    iii. Develop a data breach response policy.

c. Implement controls to achieve and maintain HIPAA compliance
    i. Establish a program to maintain minimal compliance with HIPAA requirements.
    ii. Develop a privacy policy.
    iii. Develop a data breach response policy.

8. Telecommunications, Network Security, and Architecture

a. Implement Layered Network Security with multiple levels of protection
    i. Utilize stateful or application layer firewalls, filtering routers, packet filtering or similar devices between networks.
    ii. Implement Intrusion Detection/Prevention Systems to identify and alarm on or block unauthorized access.
    iii. Implement security information and event management (SIEM)/anomaly detection to provide real-time monitoring of all PCS equipment and enterprise systems.

b. Implement network separation
    i. Implement physical (e.g. dedicated hardware) and/or logical separation (IP subnets, VLANs) to protect sensitive functions:
        1. Between PCS, enterprise systems, and other networks.
        2. Within PCS and enterprise systems:
            a. Servers
            b. HMI
            c. Field equipment
            d. Network management
            e. Third party controlled equipment
        3. Over shared communications equipment or links

c. Implement port-level security on all network devices.

d. Evaluate the risks and benefits of “pulling the plug” between PCS and the outside world.

e. Develop an architecture that will allow critical operations to continue if isolated.

f. Implement network management system to monitor system performance and identify potential bottlenecks.

g. Document and periodically review PCS network architecture and enterprise system network architecture (including definition of network boundaries).

9. Physical Security of PCS Equipment

a. Control access to:
    i. Unused network ports
    ii. Removable media
    iii. Equipment cabinets and closets
    iv. Control room
    v. Facilities
    vi. Communications pathways

10. Service Level Agreements

a. Identify all external dependencies and establish written Service Level Agreements and support contracts with internal and external support organizations to clearly identify expectations for response time and restoration of shared or leased network infrastructure and services, including equipment or services provided by:
    i. Equipment or service managed by IT departments
    ii. PCS vendors
    iii. Telecommunications and Internet providers
    iv. Power sources/power supply (within facilities)
    v. System vendors
    vi. System integrators
b. Leverage procurement policies to limit number of external support organizations.
c. Establish SLA's with staff and contracted employees for responsiveness and agreement to respond in emergency conditions.

11. Operations Security (OPSEC)

a. Provide clear demarcation between business and PCS functions. Isolate all non-PCS functions and block access from PCS equipment to:
    i. Internet browsing
    ii. Email
    iii. Any other non-PCS access to remote systems or services
b. Implement mobile device and portable media controls.

12. Cyber Informed Engineering

a. Conduct a consequence / impact analysis to prioritize scenarios.
b. Design and implement a system architecture to limit the potential impacts of an attack.
c. Include engineered controls in addition to traditional IT controls.
d. Simplify system design to the extent practical.
e. Conduct resilience planning to improve response and recovery actions.
f. Control information on the engineering of the system to prevent unwanted distribution.
g. Control procurement processes.

h. Control system interdependencies.
i. Establish and maintain a cyber-aware culture of employees, contractors, and visitors.
j. Complete a digital asset inventory to document hardware, software, and firmware currently in use.

13. Education

a. Implement a cybersecurity awareness program that includes social engineering.
b. Provide on-going cross training for enterprise system and PCS staff that identifies current best practices and standards for PCS cybersecurity.
c. Provide basic network and radio communications training for PCS technicians.
d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.
e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.
f. Provide periodic security awareness training to all employees that identifies risky behaviors and threats.
g. Promote information sharing within your organization.

14. Personnel Security

a. Implement a personnel security program for internal and contracted personnel that includes:
    i. Training
    ii. Periodic background checks
b. Require annual and new employee signoff on cybersecurity policy(ies), which includes agreeing to a confidentiality statement

AWWA Assessment Tool Output

The AWWA Assessment Tool currently produces an automatically generated output file to help utilities 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.

This output is automatically generated as a Microsoft Excel spreadsheet workbook. This file is designed to support utilities with compliance requirements of AWIA §2013. 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 your 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 utility 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 seven tabs in the file, including:

Tab 1. **Start Here** – This tab provides context and high-level instructions for the use of the output file.

Tab 2. **RRA-Control Output** – This summarizes the recommended cybersecurity controls, provides users the functionality to document the recommenced cybersecurity control status, and identifies improvement projects. This tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013. This is the only tab that requires user input.

Tab 3. **RRA – Control Status Summary** – 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. 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.

Tab 4. **ERP-Improvement Projects** – This tab provides two tables. The first is the same as the second table on tab 3. The second table is a sorted version of the controls summarized on tab 2. The intent of this second table is to allow the user to aggregate controls into projects. This table provides Priority 1 controls across each practice area. This tab is designed to facilitate compliance with the ERP requirements included in AWIA §2013. Mitigation strategies and resources may include equipment, policies and people. Once controls are aggregated into projects on this sheet, these may be grouped together using the Project Implementation Form included as tab 5.

Tab 5. **Project Implementation Form** – This is an optional sample project planning form. Full completion of the information in this form will facilitate successful project delivery.

Tab 6. **Declaration of Due Diligence** – The optional draft form is provided for use with the AWWA Assessment Tool output. The draft text is intended to facilitate communication with utility decision makers and support long-term cybersecurity risk management.

Tab 7. **User Answer Summary** – This tab provides a summary of AWWA Assessment Tool questions and associated user answers. Also included on this tab is a control status summary table. This table is presented in a "heat map" format to visually indicate the importance of controls by priority and status.

Additional details for the RRA-Control Output (Tab 3) and ERP-Improvement projects tabs (Tab 4) are provided in the following sections.

RRA-Control Output Tab

The RRA-Control Output tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013 by supporting "…assessment of the risks to, and resilience of, its system." This tab lists each of the controls recommended by the tool based on the user inputs. The recommended controls are categorized into Priorities 1, 2, 3, and 4, with Priority 1 being the highest. For each control, there are multiple columns that are available to the user to provide documentation of the level of implementation of each control at their organization.

Within this tab, the Control Status column is the only column that requires additional user input. The cells requiring input are colored blue for identification purposes. The user must select the implementation status of the recommended control within the utility/system/facility under evaluation.

The options for implementation levels include:

1. **Not Planned and/or Not Implemented** – Risk Accepted – The control is not currently implemented or planned for implementation. The organization 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.

Utility staff should use the output to document controls already in place and those that are most important to implement. This will likely require working with additional stakeholders to document the state of implementation of the various recommended controls. Improvement project categories are provided for each recommended control.

ERP-Improvement Projects Tab (Tab 4)

This tab is designed to facilitate compliance with the ERP requirements included in AWIA §2013 (b) "Emergency Response Plan", including:

- "(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."

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. This is provided in a heat map format to allow a utility to easily see a high-level control summary organized by control status and priority.

Utility staff should use this output 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.

REFERENCE STANDARDS

To provide the user with more detailed information on the steps necessary to implement the recommended cybersecurity controls, specific references to existing AWWA, NIST, and International Society of Automation (ISA) standards are provided. The references provide the specific paragraph or section number in the referenced standard in which the applicable information can be found. Table 3 provides a list of the referenced standards. Each standard listed is publicly available; however, access to several of the standards listed below require payment.

List of Standards & Guidance

	Name	Version/Revision Date
ANSI/AWWA G430-14	Security Practices for Operation and Management	November 2014
ANSI/AWWA G440-17	Emergency Preparedness Practices	August 2017
AWWA J100-10 (R13)	Risk and Resilience Management of Water and Wastewater Systems	2013
AWWA Manual M19	Emergency Planning for Water and Wastewater Utilities, Fifth Edition	2018
DHS-CAT	U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers	April 2011
DHS ICS-CERT	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies	September 2016
HIPAA	45 Code of Federal Regulations (CFR) Part 160 and Part 164	August 2002
INL CIE	Cyber-Informed Engineering	March 2017
ISA 62443-1-1	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models	October 2007
ISA 62443-2-1	Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program	January 2009
ISA TR62443-2-3-2015	Security for industrial automation and control systems Part 2-3: Patch management in the IACS environment	2015
ISA 62443-3-3	Security for industrial automation and control systems	August 2013

	Name	Version/Revision Date
	Part 3-3: System security requirements and security levels	
ISA-62443-4-1-2018	ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements	2018
ISA-62443-4-2-2018	Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components	2018
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	October 2013
ISO/IEC 27003	Information technology — Security techniques — Information security management system implementation guidance	February 2010
ISO/IEC 27005	Information technology — Security techniques — Information security risk management	June 2011
PCI-DSS v3.2.1	Payment Card Industry – Data Security Standard	May 2018
NIST Cybersecurity Framework	Cybersecurity Framework v1.1	April 2018
NIST 800-34r1	Contingency Planning Guide for Federal Information Systems	May 2010
NIST 800-53r4	Security and Privacy Controls for Federal Information Systems and Organizations	April 2013
NIST 800-61r2	Computer Security Incident Handling Guide	August 2012
NIST 800-82r2	Guide to Industrial Control Systems (ICS) Security	May 2015
NIST 800-124r1	Guidelines for Managing the Security of Mobile Devices in the Enterprise	June 2013
NIST 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	April 2015
Various	State specific data breach laws	Various

Appendix A: America's Water Infrastructure Act (AWIA) of 2018 §2013

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.

Appendix B: Network Architecture Reference Diagram and Definitions

PCS and enterprise system architecture provides an extensive list of new terminology for users of this guidance document and AWWA Assessment Tool to learn and understand. The Industrial Control System – Computer Emergency Response Team (ICS-CERT) has provided an exceptional resource for PCS owners and operators to refer to. The secure architecture design in Figure 3[12] "is the result of an evolutionary process of technology advancement and increasing cyber vulnerability presented in the Recommended Practice document, *Control Systems Defense in Depth Strategies*."[13] While this is specifically directed at PCS owners and operators, much of the terminology is compatible with enterprise systems.

[12] ICS-CERT. *Secure Architecture Design*. https://ics-cert.us-cert.gov/Secure-Architecture-Design#nogo. Last accessed May 1, 2019

[13] DHS. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf. Last accessed May 1, 2019. September 2016.

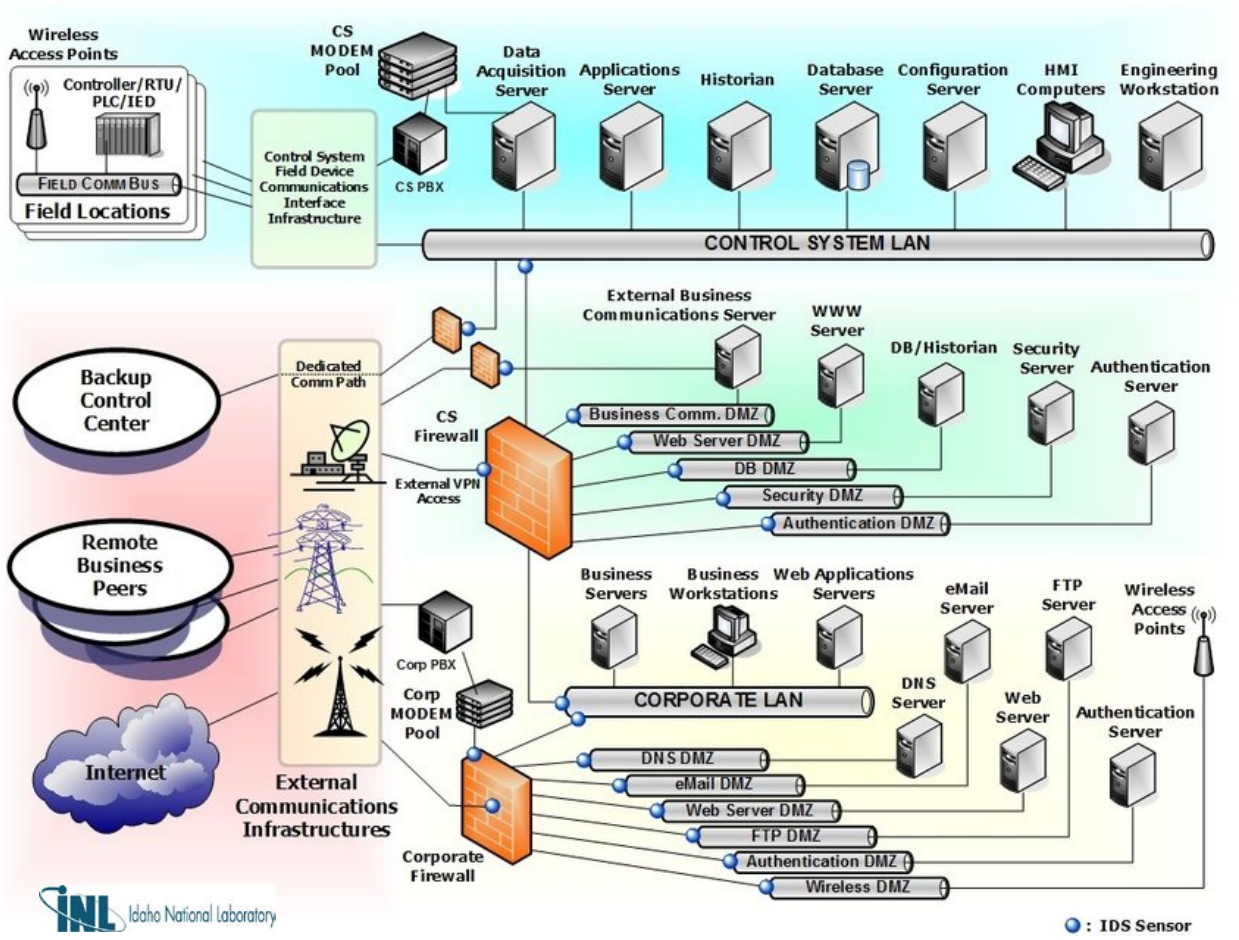

Figure 3. Secure Architecture Design

Appendix C: User Interface Questions

#	Question	Additional Details	Yes /No
1	Are any data transferred to or from your PCS network, by any electronic means?	Examples of electronic data transfer include both automatic (e.g. automated export of data from the PCS environment) and manual (e.g. transfer of data to/from the PCS environment via thumb drive). Examples of data that may be transferred include: • Water quality data collected by the PCS 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 your PCS environment?	Users include anyone internal or external with access to PCS. This may include operators, technicians, and third-party consultants. Users are able to initiate transfer of data to and from the PCS. 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 your PCS 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 PCS	

#	Question	Additional Details	Yes /No
4	Are any users allowed to access your PCS environment remotely?	Users include any personnel with internal or external access to the PCS 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-PCS environment.	
5	Is remote access to your PCS network 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 your PCS 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	Do you use resources outside your organization to support and/or maintain your PCS environment?	Examples of resources outside of the organization supporting and/or maintaining your PCS 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 your organization provide PCS 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 your PCS 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 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?	• These changes/updates include any programming of logic controllers, human machine interfaces, instrumentation, or any devices involved with the PCS. • System changes or updates do not negatively impact PCS operation. • PCS 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.	
11	Does your PCS 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 PCS	

#	Question	Additional Details	Yes /No
12	Does your PCS network 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 your PCS share a LAN or WAN with non-PCS equipment?	Examples of non-PCS 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	
14	Do you use Wi-Fi within the PCS environment to transfer data in support of operations or monitoring?	• Does your PCS communication network have wireless access points? • Wi-Fi is defined in IEEE 802.11	
15	Do you use virtualization technology for your PCS?	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	

#	Question	Additional Details	Yes /No
16	Is the virtualization technology dedicated to PCS 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 PCS virtual machines. • All non-PCS virtual machines reside on non-PCS physical host(s).	
17	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?	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.	
18	Does your 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 your 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 your 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: • Utility has an internal engineering department • Utility 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 your 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 your 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 D: Cybersecurity Use-Cases

Category/ Code	Use Case	Description
Architecture		
AR1	Dedicated Process Control Network	All network and communications infrastructure is dedicated exclusively to SCADA with no equipment or communications paths shared with non-SCADA networks.
AR2	Shared WAN	Network wide-area communications infrastructure is shared with some non-SCADA networks.
AR3	Shared LAN	Network local-area communications (within control system) is shared with non-SCADA networks.
AR4	Unlicensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using unlicensed (ISM 900 MHz, 2.4 or 5 GHz) spectrum.
AR5	Licensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using licensed spectrum.
AR6	Communications via Internet	Network wide-area communications fully or partially comprised of links over Internet services using public address space.
AR7	Communications via 3rd party carrier	Network wide-area communications fully or partially comprised of links over 3rd party carrier services (e.g. cellular, Metro-E/Ethernet/LAN).
AR8	Dedicated process control server virtualization	Virtualized server infrastructure dedicated to SCADA/Process Control with no equipment shared with non-SCADA/Process Control systems.
AR9	Shared server virtualization	Virtualized server infrastructure shared between SCADA/Process Control and non-SCADA/Process Control systems.
AR10	802.11 Wireless used in Control System	802.11 unlicensed wireless technologies used within control system.
AR11	Connection to non-SCADA Network	Connection to non-SCADA network through direct connection or firewall/DMZ.
Network Management & System Support		
NM1	Local network management and system support by SCADA/Process Control personnel in physical proximity of equipment	Access to configure network infrastructure located in immediate vicinity of user (serial or network) by SCADA/Process Control personnel.
NM2	Plant network management and	Access to configure network equipment located on same facility from centralized location by SCADA/Process Control personnel.

Category/ Code	Use Case	Description
	system support by SCADA/Process Control personnel	
NM3	Remote network management and system support by SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by SCADA/Process Control personnel.
NM4	Local network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in immediate vicinity of user (serial or network) by non-SCADA/Process Control personnel.
NM5	Plant network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in another physical facility by non-SCADA/Process Control personnel.
NM6	Remote network management and system support by non-SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by non-SCADA/Process Control personnel.
Program Access		
PA1	Outbound messaging	Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.
PA2	Outbound file transfer	Interactive sending of files from system to other locations by user.
PA3	Inbound file transfer	Interactive receiving of files from other locations to system by user.
PA4	Software updates	Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.
PA5	Data exchange	Automated, non-interactive exchange of data (e.g. database-to-database exchange, ntp or other external data) with systems located externally. (Implies full-time connection.)
PA6	Network management communications	Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)

Category/ Code	Use Case	Description
PLC Programming and Maintenance		
PLC1	Local PLC programming and maintenance	Access to PLC programming and maintenance is local to device (serial or network).
PLC2	Plant PLC programming and maintenance	Access to PLC programming and maintenance from a centralized on-site location.
PLC3	Remote PLC programming and maintenance	Access to PLC programming and maintenance from an off-site location.
PLC4	Third party SCADA/Process Control presence	SCADA/PCS equipment (e.g. PLC, RTU) owned and operated by third party (e.g. business partner) located on SCADA/Process Control network with external access by third party.
PLC5	Third party SCADA/Process Control package systems	SCADA/PCS sub-systems owned and operated by third parties located within plant facility with direct network connection to SCADA/Process Control system (package system) with on-site access by third party.
User Access		
UA1	Control room system access with control	Access to system with full read-write capability from on-plant, physically-secure “control room” location.
UA2	Plant system access with control from fixed locations	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).
UA3	Remote system access with control from fixed locations	Access to system with full read-write and/or read-only/view-only capability from location outside “control room” environment and located outside the physical perimeter of the facility workstations or HMI.
UA4	Remote system access with web view from fixed locations	Access to web displays of system data with read-only/view capability from location outside “control room” environment and located outside the physical perimeter of the facility via web browser on non-dedicated computer.
UA5	Plant system access with control from mobile device	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor) on mobile device.
UA6	Remote system access with control from mobile device	Access to system with full read-write capability from location outside “control room” environment and located outside the physical perimeter of the facility on mobile device.
UA7	Remote system access with	Access to system with limited read-only/view capability from location outside “control room” environment and located outside the physical perimeter of the facility on mobile device.

Category/ Code	Use Case	Description
	view-only from mobile device	
UA8	Remote system access with web view from mobile device	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated mobile device.
UA9	Training environment	System training conducted on production SCADA/Process Control system by third parties.
UA10	Development environment by SCADA/Process Control staff	System development conducted on production SCADA/Process Control network by SCADA/Process Control personnel.
UA11	Development environment by external staff or third parties	System development conducted on production SCADA/Process Control network by non-SCADA/Process Control personnel.
Data Security		
DS1	Accept, store or process credit card information	Organization accepts, processes, stores, or transmits credit or debit card information or certain pre-paid payment cards.
DS2	Storage of PII	Organization owns, licenses, acquires or maintains PII.
DS3	Storage or maintenance of protected health information that is HIPAA protected.	Organization creates or receives protected health information.
Cyber Informed Engineering		
CIE1	Engineering design and implementation of critical infrastructure.	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threat during the design and implementation phase.
Supply Chain		
SU1	Supply chain risk management program	Organization has a supply chain risk management program.
SU2	Supply chain risk management program cybersecurity.	Organization's supply chain risk management process addresses cybersecurity.

Appendix E: Cybersecurity Controls

AT: Awareness and Training		***Cybersecurity Practice Areas/Recommended Projects***	***Additional Details***
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	An operator finds a USB media device. Based on their cybersecurity training, they know not to use it on the company network.
AT-2	Job-specific security training including incident response training for employees, contractors and third-party users.	Education; Cyber-Informed Engineering	An operator has received what they believe to be a malicious email. They recognize that it is a phishing attack based on security training awareness programs the company has in place.
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	A SCADA tech believes a machine is infected. Based on their training, they remove the machine from the network and report it to Information Technology Team (IT) without powering it off to avoid deleting evidence.
AU: Audit and Accountability		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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	IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies.
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	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
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	Data security policy and controls are in place to prevent sharing of private or sensitive data outside of the organization.
AU-4	Information security responsibilities defined and assigned.	Governance and Risk Management	All staff are aware of who they would report to if they notice suspicious behavior in the system.

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	The facility has a documented and tested contingency plan to operate the facility without the use of SCADA software, in the case of attack by ransomware.
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	The business continuity plan is revised annually. Revisions are informed by planned exercises, actual events, or documented changes.
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	Business Continuity and Disaster Recovery	The PCS has a testing/development environment to allow changes to be implemented without immediate effects to the production environment.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Governance and Risk Management	Reviews of the organization's confidentiality/non-disclosure agreements are periodically scheduled by a responsible party.
CM: Configuration Management		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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	Meetings are periodically scheduled between management and IT to discuss current and potential cybersecurity risks and the impact on business decisions.
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.	Governance and Risk Management	The Emergency Response Plan is stored in a central repository and clearly displays the version and date of when it was implemented.
CM-3	Separation of duties implemented for user processes including risk of abuse.	Application Security; Governance and Risk Management	Operators are only given clearance to areas they are expected to work in. Supervisors have the ability and training to monitor SCADA tech activities in the PCS.
CM-4	Separation of duties implemented for development, production, and testing work.	Application Security; Personnel Security; Governance and Risk Management	A SCADA technician must have a second technician review changes made to production equipment before they are implemented.
CM-5	SLAs for all third parties established, including levels of service and change controls.	SLA	A security policy that outlines which access permissions are distributed to third party employees.
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Governance and Risk Management	Inviting all affected parties to discussions to prevent the development of vulnerabilities in the facility.
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	IT monitors SCADA computers for processor usage that could indicate cryptojacking activity.

A: Identification and Authentication & Access Control		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
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	Based on their knowledge of access control policies, operators do not share passwords.
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	Upon staff termination or resignation, login credentials are disabled as part of the Human Resources process.
IA-3	Role based access control system established including policies and procedures.	Access Control; Application Security; Governance and Risk Management	SCADA software implements unique usernames and passwords with different levels of control based on roles.
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	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
IA-5	Access control for diagnostic tools and resources and configuration ports.	Access Control	PLC programming software is only available at select workstations and only accessible to SCADA technicians.
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	Contracts with third-party equipment vendors establish security requirements for remote access to equipment.
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	To use the plant guest network, users are required to accept a user agreement.
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	Governance and Risk Management	An operator misplaces a managed phone. Based on the missing equipment policy, they contact IT to report the device lost.
IA-9	Multifactor authentication system established for critical areas.	Access Control	Remote access to the SCADA system requires two factor-authentication.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Governance and Risk Management	Idle sessions on SCADA screens are logged off in 15 minutes. If no user is logged in, a read-only view is presented.
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high-risk locations.	Access Control	The controls to critical equipment are only available at a local secured terminal.
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	Access Control	An operator attempts to connect to a known hacking website. The connection is blocked. The operator and IT are notified of the attempt.

IR: Incident Response, Contingency Planning, & Planning		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
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	Emergency Response Plan includes procedures for recovering SCADA system operation from system backup.
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	A SCADA tech believes a machine is infected and responds according to the utility's emergency response plan for cybersecurity based incidents.
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	The Emergency Response Plan is reviewed and updated once a year by responsible staff.
MA: Maintenance		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Service Level Agreement Governance and Risk Management; Cyber-Informed Engineering	Based on the company's controlled maintenance program, a utility will format network devices to factory settings before sending them out of the organization for maintenance.
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	The utility is a member of DHS's ICS-CERT mailing list to receive frequent communications on PCS vulnerabilities discovered and patches available. SCADA techs regularly review alerts to determine if the alerts are applicable to their system.
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	Governance and Risk Management	The condition of offsite equipment and risk factors acting on the equipment are periodically reviewed and assessed via an independent party.

MP: Media Protection		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
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	When decommissioning a network device that was used in the production environment, IT is required to return it to factory conditions before it leaves the facility.
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	Governance and Risk Management	The Emergency Response Plan is stored in a central repository that records when files are accessed and altered.
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Governance and Risk Management	Company policies and procedures are available in a central, secure, shared location.
PE: Physical and Environmental Protection		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
PE-1	Security perimeters, card-controlled gates, manned booths, and procedures for entry control.	Access Control; Physical Security	Personnel are required to present a badge to access the PCS.
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Access Control; Physical Security	Access to the server room is restricted to authorized staff only.
PE-3	Physical security and procedures for offices, rooms, and facilities.	Access Control; Governance and Risk Management; Physical Security	Staff lock doors that allow access to PCS assets. Security guards inspect doors to make sure they are locked properly.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Access Control; Physical Security	Fire suppression unit installed around critical equipment.
PE-5	Physical security and procedures for working in secure areas.	Access Control; Physical Security	Documentation for physical security procedures is included with new employee training and reviewed at regular training events.
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from PCS enterprise system areas.	Access Control; Physical Security	Server room and PLC cabinets are isolated from areas that delivery personnel and customers may visit.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	Physical Security	The utility monitors facilities using security cameras.
PE-8	Physical/logical protection against power failure of equipment UPS.	Physical Security; Service Level Agreements	Uninterruptible power supplies (UPS) are available as power backup for critical components.
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	Physical Security	A utility has a standby power source with separated power cabling for critical sites.

PM: Program Management & Security Assessment and Authorization		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
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	A database is used to keep track of building conditions in the facility.
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	Governance and Risk Management;	PLCs that cannot update past a specific security revision are not acceptable for use in the PCS.
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;	A utility has a network intrusion detection system (NIDS) to monitor network traffic.
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	Third parties must review and sign an information exchange policy before connecting to the system.
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	Governance and Risk Management	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies the integrator of the secure file transfer system in place.
PS: Personnel Security		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
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	A background check on employees is required before they may be given access to the PCS system.
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third-party users.	Governance and Risk Management; Personnel Security	A company policy is in place limiting the access of third-party users to assets, systems, and data.
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.	Governance and Risk Management; Personnel Security	Confidential documents are stored in locked file cabinets when not in use, as required by policy.
PS-4	Disciplinary process for security violations established.	Governance and Risk Management; Personnel Security	An operator who props open doors to critical areas could face disciplinary action as outlined in the utility's policies and procedures.

RA: Risk Assessment		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	Governance and Risk Management	A third-party system integrator would need to contact IT before connecting to the system's network.
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	System integrators can only access the facility's equipment remotely from a Virtual Private Network (VPN) connection.
SA: System and Services Acquisition		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
SA-1	Authorization process established for new systems or changes to existing information processing systems.	Governance and Risk Management	A change management/review process is used to evaluate suggested changes to facility.
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	A third-party system integrator is preparing to make changes to SCADA software. The SCADA tech requires the integrator to follow the change procedure and test the changes in a sandbox environment before they are deployed in production.
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	Automatic updates to the operating system are disabled, but monthly manual updates are reviewed and applied in coordination with operations.
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	Remote access is restricted to only the most necessary applications and only allowed through secure measures.
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	Governance and Risk Management	System backups are tested on a regular basis by completing a system restoration to the test environment.
SI: System and Information Integrity		*Cybersecurity Practice Areas/ Recommended Projects*	*Additional Details*
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	The company selected to perform billing is compliant with pertinent laws, regulations, policies and procedures that are relevant to the utility.
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	Acquired assets are inspected, assessed, and documented before implementation with existing systems.

SI-3	Interactive system for managing password implemented to ensure password strength.	Access Control; Application Security	When configuring a new user's password, it must meet minimum character length requirements.
SI-4	Organization-wide clock synchronization system in place.	Telecommunications, Network Security, and Architecture	All managed network devices synchronize their clocks to a known good source.
SI-5	Privileged programs controls established to restrict usage of utility 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	Utility has implemented tiered access so non-administrator users are unable to make changes to system security settings.
DS: Data Security		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
DS-1	A program established to ensure compliance with the minimum PCI requirements for your associated level.	Governance and Risk Management; Data Security	The company selected to perform billing is compliant with the minimum PCI requirements for the utility's associated level.
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	An operator knows how to identify and respond to a suspected cyber breach, based on their cybersecurity training.
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	Current practices are reviewed by legal counsel for legal compliance with HIPAA.
CIE: Cyber-Informed Engineering		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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	Engineering staff is fully aware of the potential for a cyber breach. They design electrical and mechanical systems to provide functionality in the case of a SCADA system compromise.
SU: Supply Chain		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
SU-1	A supply chain risk management program.	Governance and Risk Management	Chain of custody documentation is required for all chemicals used in treatment.
SU-2	A supply chain risk management program that includes cybersecurity.	Governance and Risk Management	Preferred vendors for computer hardware, software and peripherals are identified and selected based on evaluation of their supply chain among other criteria.

SC: System and Communications Protection		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
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	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communication.
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Access Control; Application Security	Operators have one username and password for PCS equipment which is managed from a central system.
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	All external communication with the PCS is implemented via DMZ.
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	Within the SCADA system network, vendor systems are placed on a separate subnet.
SC-5	Anomaly based IDS/IPS established including policies and procedures.	Telecommunications, Network Security, and Architecture	The IT tech monitors IDS system exception logs daily to determine if ongoing attacks are occurring and works with SCADA tech to address any issues.
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	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
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	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communications.
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	Within the SCADA system network, vendor systems are placed on a separate subnet rather than being on a single "flat" network.
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	A utility will physically separate a pump station from any sort of information transfer from any other network. This however is only a true air gap when there is absolutely no information transfer. If information is transferred though a DMZ or firewall that would not be an example of this control. In that scenario select this control as “Not Planned and/or Not Implemented - Risk Accepted”.

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	Ports are disabled for all network devices when not in use.
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	A water utility chooses to not allow personal mobile devices to connect to the control network. The utility does provide mobile devices managed by IT that can connect to the network.
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	Remote access to the SCADA system requires two factor-authentication.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Governance and Risk Management	Organization has a FAT procedure that requires vendors to demonstrate security of systems before they are purchased.
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	Operations Security; Telecommunications, Network Security, and Architecture	"Whitelisting" of network components is done to manage data transfer between and within network segments.
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	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	Operations Security; Telecommunications, Network Security, and Architecture	A utility employs multiple types of physical and cybersecurity efforts to protect assets and systems. The efforts include such things as locking doors, physical access control, and unique login requirements for each staff member.
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are on a separate subnet.
SC-18	Minimize wireless network coverage.	Telecommunications, Network Security, and Architecture	Tests are conducted regularly to determine if the WiFi signals reach outside the intended area of use. If the signal reaches outside the intended area, the signal is turned down accordingly.
SC-19	802.1X user authentication on wireless networks.	Telecommunications, Network Security, and Architecture	No "open" WiFi connections are allowed.
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.	Telecommunications, Network Security, and Architecture	WiFi equipment in the plant does not connect directly to SCADA network.
SC-21	Unique wireless network identifier SSID for control network.	Telecommunications, Network Security, and Architecture	The WiFi for the control system has a unique SSID from the business network.

SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	Telecommunications, Network Security, and Architecture	A wireless LAN specific domain controller is in place.
SC-23	Wireless communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture	All data transferred via the wireless network is encrypted using current wireless communication best practices.
SC-24	Communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture	All data transferred via the wired network is encrypted using current wireless communication best practices.
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	An operator who can access the system remotely must do so through a secured VPN client configuration.

Appendix F: Cross Reference to NIST 1.1 Cybersecurity Framework

The following table provides a cross-reference between the Cybersecurity Controls incorporated into the AWWA Cybersecurity Guidance Tool and the Framework Core (Appendix A) included in the Cybersecurity Framework issued by NIST on April 16, 2018.

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY	Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried	PM-2
		ID.AM-2	Software platforms and applications within the organization are inventoried	PM-2
		ID.AM-3	Organizational communication and data flows are mapped	PM-2
		ID.AM-4	External information systems are catalogued	MA-3
		ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	PM-5
		ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	PE-4, PS-2
	Business Environment	ID.BE-1	The organization's role in the supply chain is identified and communicated	RA-2, PS-2, CM-5
		ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	MA-2
		ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	IR-2
		ID.BE-4	Dependencies and critical functions for delivery of critical services are established	IR-2
		ID.BE-5	Resilience requirements to support delivery of critical services are established	IR-3
	Governance	ID.GV-1	Organizational information security policy is established	IR-2, AU-2
		ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PS-2, AU-4, AU-6
		ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	IR-3
		ID.GV-4	Governance and risk management processes address cybersecurity risks	AU-3, AU-5, CM-6
	Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented	AU-5, RA-1, IR-2
		ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	AU-5, PM-3, IR-2

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY – cont'd		ID.RA-3	Threats, both internal and external, are identified and documented	AU-5, RA-1, IR-2
		ID.RA-4	Potential business impacts and likelihoods are identified	AU-5, RA-1, IR-2
		ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	AU-5
		ID.RA-6	Risk responses are identified and prioritized	IR-1
	Risk Management Strategy	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	IR-2
		ID.RM-2	Organizational risk tolerance is determined and clearly expressed	SA-4
		ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	SC-4
	Supply Chain Risk Management	ID.SC-1:	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SU1
		ID.SC-2:	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	SU2
		ID.SC-3:	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	SU2
		ID.SC-4:	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	SU1
PROTECT	Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users	IA-1, RA-1, SC-19
		PR.AC-2	Physical access to assets is managed and protected	PE-1, PE-2, PE-3
		PR.AC-3	Remote access is managed	IA-7, SC-12, SC-18, SC-21, RA-2
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	IA-3, SC-22
		PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	SC-8, SC-9, SC-14, SC-15, SC-16, SC-17, SC-20, SC-25

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*	Awareness & Training	PR.AT-1	All users are informed and trained	AT-1, AT-2
		PR.AT-2	Privileged users understand roles & responsibilities	AT-1, AT-2
		PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	AT-2
		PR.AT-4	Senior executives understand roles & responsibilities	AT-1
		PR.AT-5	Physical and information security personnel understand roles & responsibilities	PS-4, AT-1
	Data Security	PR.DS-1	Data-at-rest is protected	PM-5, MP-2
		PR.DS-2	Data-in-transit is protected	PM-4, SC-14, SC-23, SC-24
		PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	PM-1
		PR.DS-4	Adequate capacity to ensure availability is maintained	MA-1, CM-7
		PR.DS-5	Protections against data leaks are implemented	IA-4
		PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	IR-3
		PR.DS-7	The development and testing environment(s) are separate from the production environment	CM-4
	Information Protection Processes and Procedures (IP)	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained	SA-3
		PR.IP-2	A System Development Life Cycle to manage systems is implemented	CM-1, CM-6
		PR.IP-3	Configuration change control processes are in place	SA-3
		PR.IP-4	Backups of information are conducted, maintained, and tested periodically	SA-5
		PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	PE-4
		PR.IP-6	Data is destroyed according to policy	MP-1
		PR.IP-7	Protection processes are continuously improved	AU-6
		PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	AU-7
		PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	ANSI/AWWA J100/G440/M19
		PR.IP-10	Response and recovery plans are tested	PS-4

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*		PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	AT-2
		PR.IP-12	A vulnerability management plan is developed and implemented	AU-5
	Maintenance	PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-1
		PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-1
	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PM-3
		PR.PT-2	Removable media is protected and its use restricted according to policy	MP-1
		PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality (whitelisting)	SC-10, SC-19
		PR.PT-4	Communications and control networks are protected	IA-7
DETECT	Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	Not addressed
		DE.AE-2	Detected events are analyzed to understand attack targets and methods	SC-5
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	Not addressed
		DE.AE-4	Impact of events is determined	PM-3
		DE.AE-5	Incident alert thresholds are established	CM-7
	Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events	CM-7
		DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	PE-1, CM-7
		DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	CM-7, SA-5
		DE.CM-4	Malicious code is detected	SC-5
		DE.CM-5	Unauthorized mobile code is detected	SA-4
		DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	IA-2
		DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	PS-1
		DE.CM-8	Vulnerability scans are performed	IR-2
	Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability and adequate awareness of anomalous events	PS-2
		DE.DP-2	Detection activities comply with all applicable requirements	IR-3

Function	Category	Sub-Category	Description	AWWA Guidance Control
DETECT – *cont.*		DE.DP-3	Detection processes are tested	ANSI/AWWA G430, G440
		DE.DP-4	Event detection information is communicated to appropriate parties	IA-2
		DE.DP-5	Detection processes are continuously improved	SC-4
RESPOND	Response Planning	RS.PL-1	Response plan is executed during or after an event	AT-1
	Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed	ANSI/AWWA G430, G440
		RS.CO-2	Events are reported consistent with established criteria	G430
		RS.CO-3	Information is shared consistent with response plans	SC-6
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans	ANSI/AWWA G430, G440
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	MA-2
	Analysis	RS.AN-1	Notifications from detection systems are investigated	SC-5
		RS.AN-2	The impact of the incident is understood	ANSI/AWWA J100
		RS.AN-3	Forensics are performed	AT-3
		RS.AN-4	Incidents are categorized consistent with response plans	AT-3
	Mitigation	RS.MI-1	Incidents are contained	IR-1
		RS.MI-2	Incidents are mitigated	IR-1
		RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	IR-2
	Improvements	RS.IM-1	Response plans incorporate lessons learned	ANSI/AWWA G430, G440
		RS.IM-2	Response strategies are updated	ANSI/AWWA G430, G440
RECOVER	Recovery Planning	RC.RP-1	Recovery plan is executed during or after an event restoration of systems or assets affected by cybersecurity events	AU-7
	Improvements	RC.IM-1	Recovery plans incorporate lessons learned	ANSI/AWWA G430, G440
		RC.IM-2	Recovery strategies are updated	ANSI/AWWA G430, G440
	Communications	RC.CO-1	Public relations are managed	ANSI/AWWA G430, G440
		RC.CO-2	Reputation after an event is repaired	ANSI/AWWA G430, G440
		RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	ANSI/AWWA G430, G440

NOTES

NOTES

About AWWA

AWWA is an international, nonprofit, scientific and educational society dedicated to providing total water solutions assuring the effective management of water. Founding 1881, the Association is the largest organization of water supply professionals in the world. Our membership includes nearly 4,200 utilities that supply roughly 80 percent of the nation's drinking water and treat almost half of the nation's wastewater. Our over 50,000 total memberships represent the full spectrum of the water community: public water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource. AWWA unites the diverse water community to advance public health, safety, the economy, and the environment.