Process Control System Security Guidance for the Water Sector

American Water Works Association

Acknowledgements

Project Advisory Committee

Don Dickinson, Phoenix Contact
Melani Hernoud, Secure Network Systems LLC
Brad Jewell, Orlando Utilities Commission
Ariz Naqvi, Alameda County Water Department
Jerry Obrist, Lincoln Water

AWWA Staff

Kevin Morley

Project Contractors

Tim Payne, EMA Inc.
Philip Gaberdiel, EMA Inc.
Bob George, EMA Inc.
Rafael Alpizar, EMA Inc.
Terry Brueck, EMA Inc.
Penny Brink, EMA Inc.

Subject Matter Expert Panel

Steve Allgeier, Environmental Protection Agency
Rebecca Bace, University of South Alabama
John Brosnan, Santa Clara Valley Water District
Vic Burchfield, Columbus Water Works
Terry Draper, HDR
Michael Firstenberg, Waterfall Security Solutions
Rod Graupmann, Pima County Regional Wastewater Reclamation Department
Steve Hansen, Las Vegas Valley Water District
Elkin Hernandez, DC Water
Darren Hollified, Jacksonville Electric Authority
James Johnson, Charlotte-Mecklenburg Utilities
Lisa Kaiser, Department of Homeland Security
Kent Knudsen, K2Share
Diana McCormick, DC Water
Eric Meyers, WaterISAC
Tony Palamara, Onondaga County Water Authority
Mike Queen, Charlotte-Mecklenburg Utilities
Robert Raffaele, American Water
Michael Richardson, Cape Fear Public Utility Authority
David Robinson, Dallas Water Utilities
Cheryl Santor, MWD of Southern California
Mary Smith, Water Research Foundation
Todd Smith, Greater Cincinnati Water Works
Shannon Spence, Arcadis
Mike Sweeney, Toho Water
Joellen Thompson, City of Grand Rapids
Jacqueline Torbert, Orange County Utilities

Project Funding

This project was funded by the American Water Works Association (AWWA), utilizing the Water Industry Technical Action Fund (WITAF), WITAF Project #503.

TABLE OF CONTENTS

1.0 Executive Overview

Within the last two decades cybersecurity threats including cyber terrorism has grown from the esoteric practice of a few specialists to a problem of general concern. National infrastructures have been found to be particularly vulnerable to such attacks. In response to this threat, a number of standards organizations have produced a wide array of standards and guidelines 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)[1] from cyber-attacks. This action was very timely in that it coincided with the issuance of Presidential Executive Order 13636 – Improving Critical Infrastructure, on February 19, 2013, which directed the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure. The NIST Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The goal of the AWWA guidance is to provide water sector utility owners/operators with a consistent and repeatable 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 project is also expected to communicate a "call to action" for utility executives acknowledging the significance of securing PCS given their role in supporting water utility operations.

A panel of industry subject matter experts has been consulted to identify the most pressing cybersecurity issues facing water utilities today. In response to these issues, a list of recommended cybersecurity practices has been developed. This list identifies practices considered to be the most critical for managing the PCS cybersecurity risk in the water sector. Section 2.0 of this report provides a discussion of the Recommended Practices and why they are important to supporting a robust cybersecurity posture.

These recommended practices are further defined by a set of 82 cybersecurity controls that represent the more granular measures necessary to support implementation of the recommended practices. In an effort to provide water utilities with actionable tasks, a Cybersecurity Guidance Tool was developed to present these controls to users in a concise, straightforward manner.

The Cybersecurity Guidance Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user provides information about their process control system and the manner in which it is used by choosing from a number of pre-defined use cases. For each recommended control, specific references to existing cybersecurity standards are also provided.

The tool emphasizes actionable recommendations with the highest priority assigned to those that will have the most 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.

The AWWA Guidance and Tool represents a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council. This resource will be a living document, and further revisions and enhancements will be made based on user input.

[1] The term process control system (PCS) is preferred over industrial control system (ICS) to avoid confusion

2.0 Recommended Cybersecurity Practices

2.1 Overview

The cybersecurity practices are a set of recommendations for improving the security posture of the process control systems (PCS) used by water and wastewater utilities. They are actionable recommendations designed to produce maximum improvement in the short term, and lay the foundations for longer term implementation of complex security programs and controls.

The list of recommended practices in Table 2-1 was compiled by a panel of key industry personnel and subject matter experts (SME) in cybersecurity and other related areas. The approach used to develop the list was to combine the operational knowledge of the SME panel with best practices and information from a number of security standards from DHS, NIST, AWWA, WaterISAC, and others. The result is a comprehensive set of recommendations that can be put into practice immediately and that will quickly yield tangible results.

2.2 Practice Categories

The practice categories were chosen by SME teams during a Definition Workshop. Each team identified important areas of security to be addressed and policies, activities, and systems that should be implemented. The recommendations from each team were then 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 categories and recommendations were comprehensive. The categories (like their NIST framework counterparts) are not mutually exclusive and contain significant overlap.

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 components.

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 the management of the enterprise.

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 fast recovery after disruptions in service.

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 allowed to run in servers and workstations throughout the enterprise.

Access Control

This category is concerned with ensuring that only authorized personnel is able 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 systems that those used to access 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 SCADA system is supposed to receive data from a 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.

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 layered defense architecture with the PCS 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 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 to define, negotiate, execute, and monitor 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) services 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.

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 Facebook 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.

Table 2-1
Recommended Cybersecurity Practices for the Water Sector

1. **Governance and Risk Management**
    a. Develop a formal, written Cybersecurity Policy that addresses the specific operational needs of Process Control System(s) (PCS)
    b. Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans
    c. Perform a vulnerability assessment (CSET or physical assessment) on a regular basis.
    d. To aid in developing contingency plans, maintain current PCS asset inventory, 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 PCS hardware and software standards in order to limit number of system components
    f. Develop standard specifications language that defines PCS cybersecurity standards for inclusion in all procurement packages

2. **Business Continuity and Disaster Recovery**
    a. Develop PCS Disaster Recovery/Business Continuity Plan, including:
        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 Incident Response Plan includes procedures and contact list for PCS
    c. Implement change management program for PLC software; maintain fully commented backups for all PLC programs and test restore process on a periodic basis
    d. 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). Rename Administrator account
    g. Disable USB, DVD, and other external media ports
    h. Disable auto-scan of removable media

4. **Access Control**
    a. Secure PCS 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 PCS. Include system and software updates
            2. Data exchange between PCS and others 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 SCADA or program field devices should be "dedicated for SCADA use only" and ports to Internet disabled. All non-essential software should be removed.

5. **Application Security**
    a. Require each PCS 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 actually administering the system.
    c. Provide separate credentials for PCS access from normal business 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. **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.
    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 and other networks.
            2. Within PCS:
                a. Servers
                b. HMI
                c. Field equipment
                d. Network management
                e. 3rd 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. Develop an architecture that will allow critical operations to continue if isolated.
    e. Implement network management system to monitor system performance and identify potential bottlenecks.
    f. Document and periodically review PCS network architecture (including definition of PCS network boundaries)

8. **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

9. **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

10. **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.

11. **Education**
    a. Implement a cybersecurity awareness program that includes social engineering.
    b. Provide on-going cross training for IT 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.

12. **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 PCS Cybersecurity Policy, which includes agreeing to a confidentiality statement

3.0 Cybersecurity Guidance Tool

3.1 Overview

The guidance tool is fairly simple to use, as illustrated Figure 3-1.

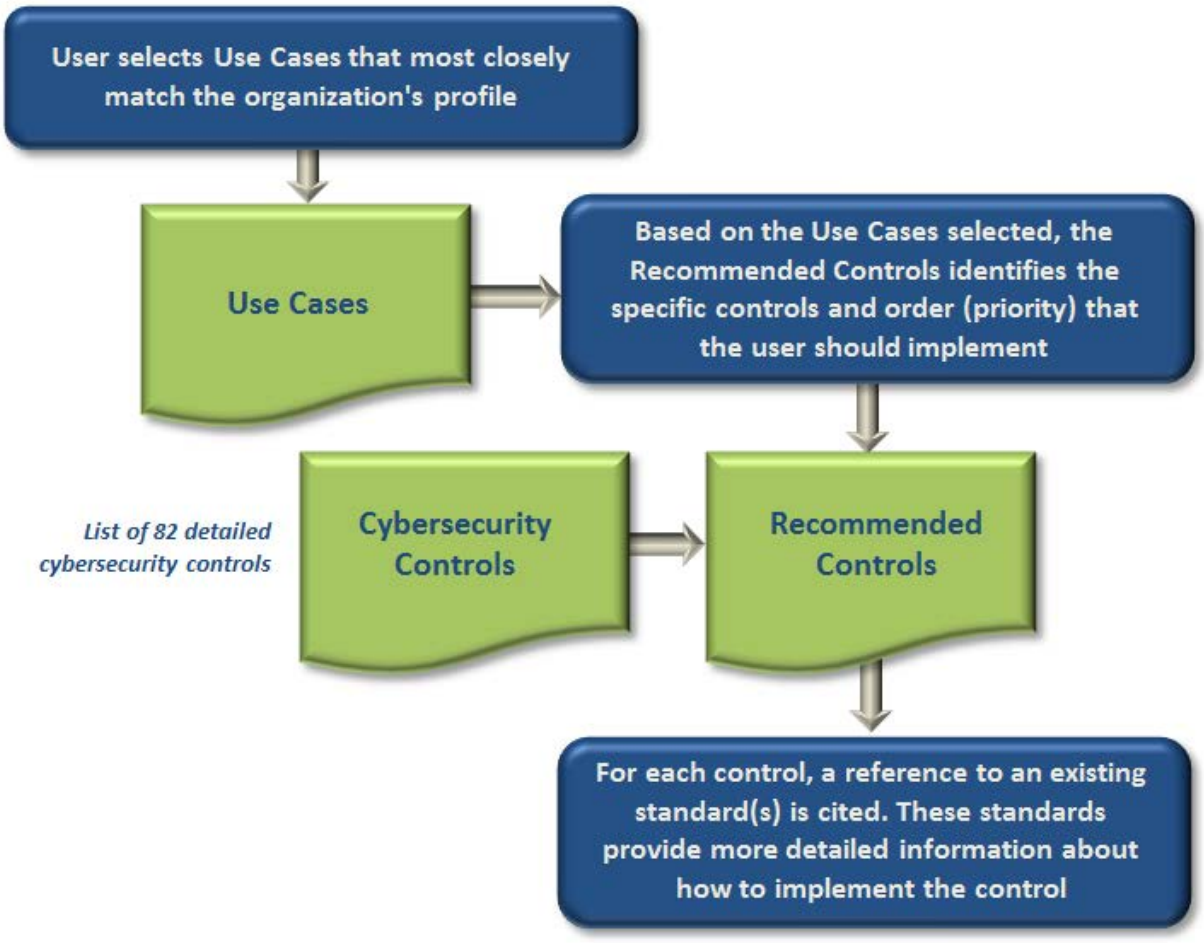

Figure 3-1
Cybersecurity Guidance Tool

The user first selects the use cases which most closely matches their utility's current cybersecurity need. See Figure 3-2. Additional information about use cases is provided in Section 3.2. Based on the use case selection, the tool identifies the most appropriate cybersecurity controls. The recommended controls are categorized by 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.

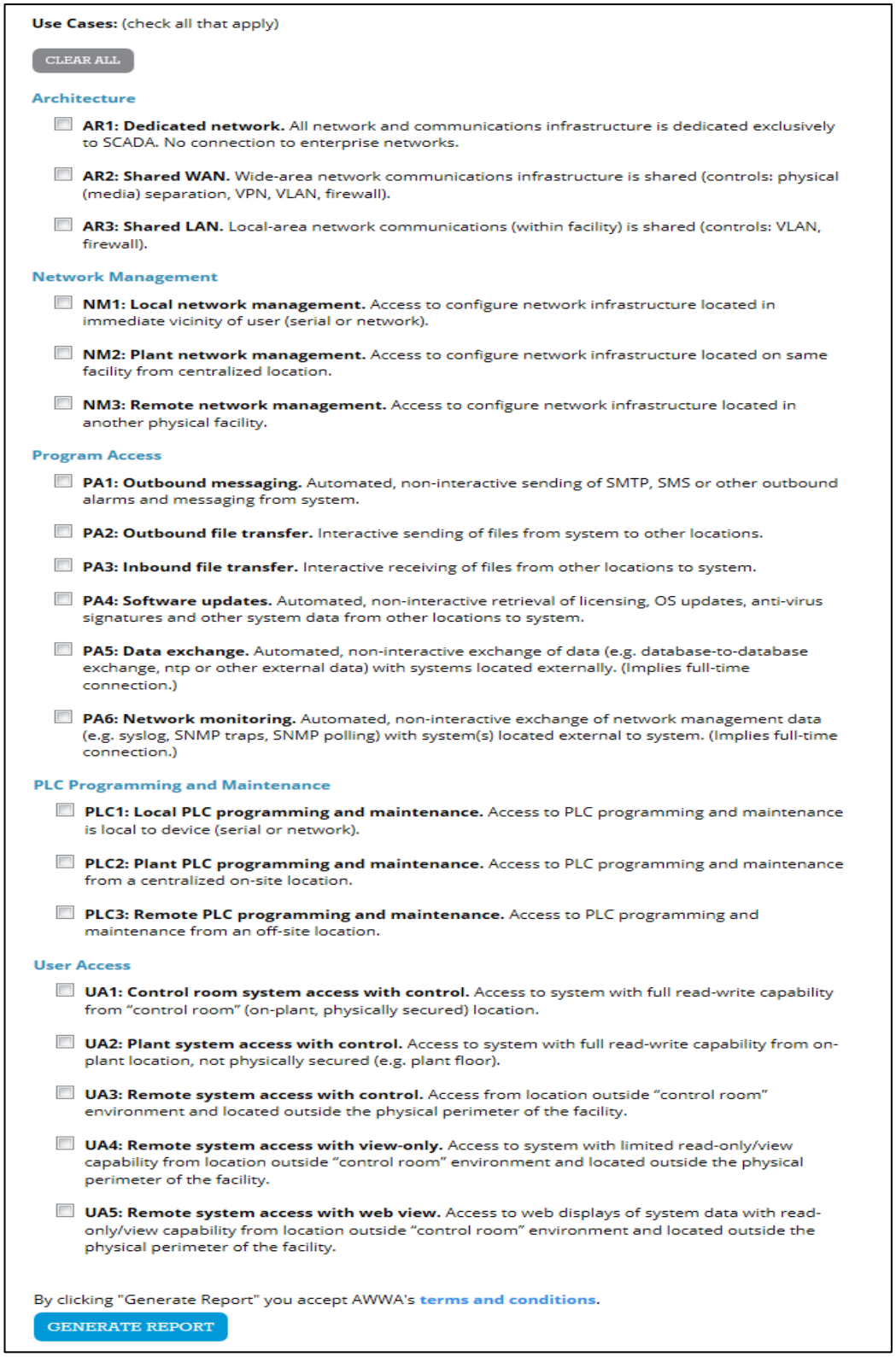

Figure 3-2
Use Cases

Figure 3-3 is an example of a priority 1 list for the Local Network Management use case. A description of the cybersecurity controls and the different priorities is provided in Section 3.3. A list of referenced standards is provided in Section 3.4.

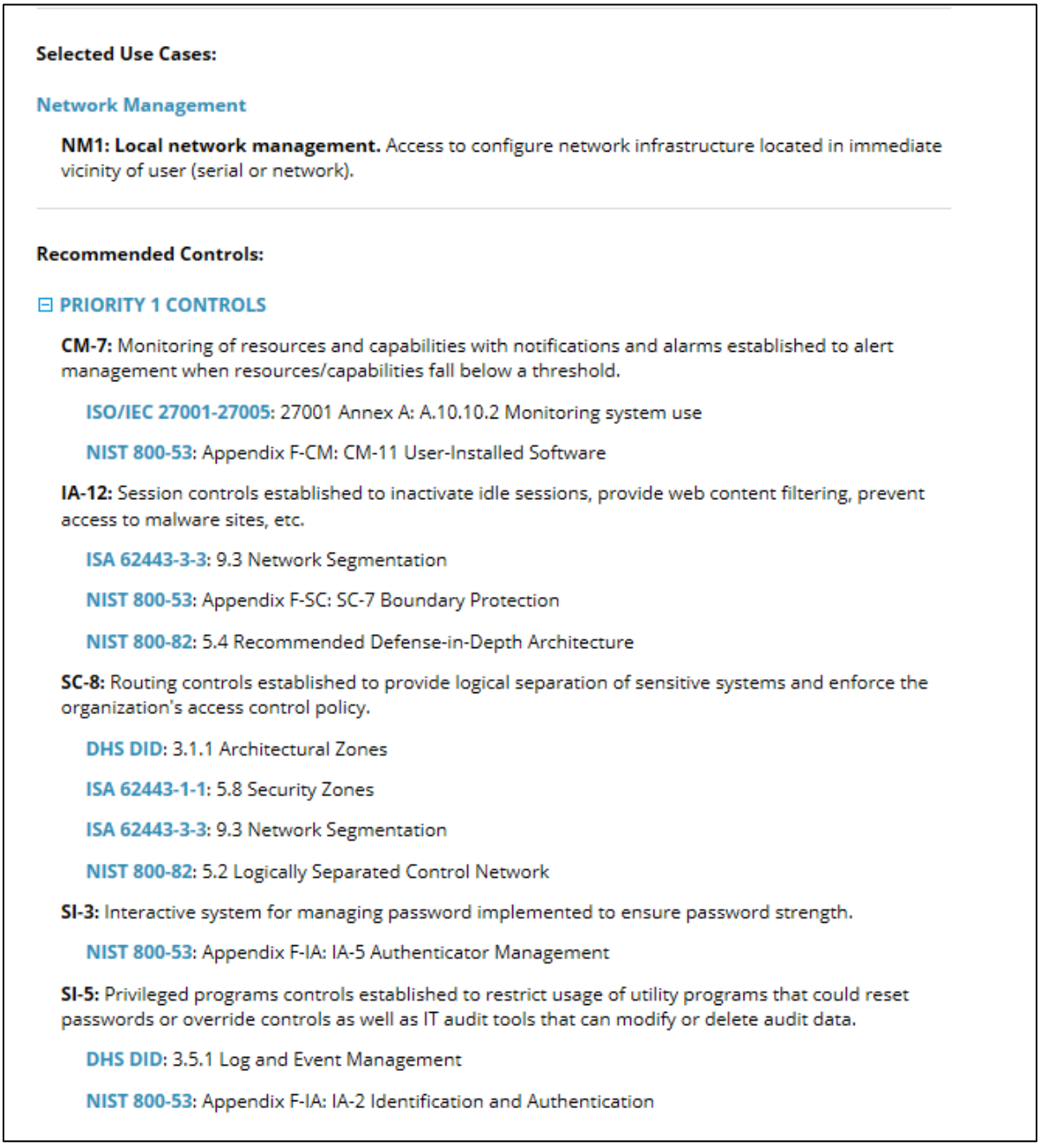

Figure 3-3
Priority 1 Controls

The Cybersecurity Guidance Tool can be used in multiple ways:

First, a user can research the security implications of implementing a procedure, changing architecture, or providing a service from the PCS network. To do this, the user selects the use case that most resembles what he wants to do and explores the results that the tool yields. The resulting controls will be grouped by priority. Priority 1 and 2 will indicate the most important controls to implement in the short term. The user can research the sources of these controls by looking at the standards-matrix which correlates the controls to the standards.

Second, a user can select all the use cases that describe his organization and by selecting the priority 1 button get a report of the top controls to implement. Users should keep in mind that a tool like this is not infallible and that a “second opinion” based on an in-depth understanding of an organization’s current security posture as well as business goals should be considered before proceeding.

Third, if an organization has already addressed the recommended priority 1 and 2 controls, they should begin to lay a security framework in order to build a comprehensive security program. The lowest priority controls (3 and 4) typically apply to the entire organization and are usually related to governance. Implementing these controls under a governance framework, like ISO 27001 or NIST 800-52, is the best way to establish a long term security program.

3.2 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 description of important processes within PCS from the user's perspective.

Table 3-1 provides a brief description of each use case and why it leads to different considerations for cybersecurity.

Table 3-1
Use Cases

Category/ Code	Use Case	Description	Security Considerations
User Access			
UA1	Control room system access with control	Access to system with full read-write capability from "control room" (on-plant, physically secured) location.	Minimal access control needed here. Other issues like thumb drives and DVD usage may become a problem.
UA2	Plant system access with control	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).	Medium network security needed here. Other issues like thumb drives and DVD usage may become a problem.
UA3	Remote system access with control	Access from location outside "control room" environment and located outside the physical perimeter of the facility.	Very rigorous access control and monitoring needed to authenticate remote users. Network topology is an issue; control of traffic into PCS network is needed.
UA4	Remote system access with view-only	Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.	Special one way controls are needed. One way data flow can be done by ACLs or specialized equipment.
UA5	Remote system access with web view	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.	High network security needed. Network topology is an issue; control of traffic into PCS network is needed.
PLC Programming and Maintenance			
PLC1	Local PLC programming and maintenance	Access to program PLC located in immediate vicinity of user (serial or network).	Recommended practice.
PLC2	Plant PLC programming and maintenance	Access to program PLC located on same facility from centralized location.	Careful implementing authentication.
PLC3	Remote PLC programming	Access to program PLC located in another physical facility.	Not a recommended practice; two factor authentication should be in place. Dangerous!
Network Management			
NM1	Local network management	Access to configure network infrastructure located in immediate vicinity of user (serial or network).	Basic access control needed. Network equipment managed from SCADA facilities only, over SCADA network infrastructure
NM2	Plant network management	Access to configure network infrastructure located on same facility from centralized location.	Medium security needed.
NM3	Remote network management	Access to configure network infrastructure located in another physical facility.	High security needed. High reliability on authentication of users.

Table 3-1 (cont.)
Use Cases

Category/ Code	Use Case	Description	Security Considerations
Program Access			
PA1	Outbound messaging	Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.	Routing and ACL restrictions, network topology reconsidered to ensure only outbound messages.
PA2	Outbound file transfer	Interactive sending of files from system to other locations.	Routing and ACL restrictions, network topology reconsidered to ensure only outbound messages.
PA3	Inbound file transfer	Interactive receiving of files from other locations to system.	Very high security and monitoring needed. Concern with file content. .
PA4	Software updates	Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.	Very high security and monitoring needed. Concern with file content. Certificate monitoring and deep packet inspection can be used to detect issues.
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.)	Encapsulation of data flows in a secure channel. Monitoring of payload for unusual data.
PA6	Network authentication	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.)	Very high security and monitoring needed. SNMP security is a concern. Appropriate securing of SNMP is needed.
Architecture			
AR1	Dedicated Network	All network and communications infrastructure is dedicated exclusively to SCADA (controls: network segmentation).	Low network security needed here. Other issues like thumb drives and DVD usage may become a problem.
AR2	Shared WAN	Network wide-area communications infrastructure is shared (controls: physical (media) separation, VPN, VLAN, firewall)	High security and monitoring needed. Network topology is an issue; control of traffic into PCS network is needed.
AR3	Shared LAN	Network local-area communications (within facility) is shared (controls: VLAN, firewall)	Very high security and monitoring needed. Authentication of users accessing PCS.

3.3 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 controls which were similar were merged into a single, more comprehensive control. Some controls are complex and might resemble an administrative program or a computer system. Indeed many software companies develop computer systems to implement controls of greater complexity (e.g., network monitoring tools). Table 3-2 provides a complete list of the cybersecurity controls developed for this document.

Each control was assigned a priority level based on its criticality and potential impact to the security of the utility. Priority levels are defined as follows:

- **Priority 1 Controls** – These controls represent the minimum level of acceptable security for SCADA/PCS. If not already in place, these controls should be implemented immediately.
- **Priority 2 Controls** – These controls should be implemented second because they have the potential to provide a significant and immediate increase in the security of the organization.
- **Priority 3 Controls** – These controls provide additional security against cybersecurity attack of PCS Systems and lay the foundation for implementation of a managed security system. These controls should be implemented as soon as budget allows.
- **Priority 4 Controls** – These controls are more complex and provide protection for more sophisticated attacks (which are less common); they also provide for managed security systems. Many Priority 4 controls are related to policies and procedures; others involve state-of-the-art protection mechanisms. They are important for a complete program as they may offer critical protection against a sophisticated, targeted attack.

Table 3-2
Cybersecurity Controls

AU: Audit and Accountability	
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.
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.
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.
AU-4	Information security responsibilities defined and assigned.
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.
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.
RA: Risk Assessment	
RA-1	Risk assessment and approval process before granting access to the organization's information systems.
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.
CA: Security Assessment and Authorization ***PM: Program Management***	
PM-1	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.
PE: Physical and Environmental Protection	
PE-1	Security perimeters, card controlled gates, manned booths, and procedures for entry control.
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.
PE-3	Physical security and procedures for offices, rooms, and facilities.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.
PE-5	Physical security and procedures for working in secure areas.
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from IT/PCS areas.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.
PE-8	Physical/logical protection against power failure of equipment (UPS).
PE-9	Physical/logical protection against access to power and telecommunications cabling established.

Table 3-2 (cont.)
Cybersecurity Controls

PS: Personnel Security	
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.
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third party users.
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.
PS-4	Disciplinary process for security violations established.
MA: Maintenance	
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized.
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.
MP: Media Protection	
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).
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.
MP-3	Policies and procedure repository in place to be available to all authorized staff.
CM: Configuration Management	
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.
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.
CM-3	Separation of duties implemented for user processes including risk of abuse.
CM-4	Separation of duties implemented for development, production, and testing work.
CM-5	SLAs for all third parties established, including levels of service and change controls.
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.
SA: System and Services Acquisition	
SA-1	Authorization process established for new systems or changes to existing information processing systems.
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.
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.
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.

Table 3-2 (cont.)
Cybersecurity Controls

AC: Access Control	
IA: Identification and Authentication	
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.
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.
IA-3	Role based access control system established including policies and procedures.
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).
IA-5	Access control for diagnostic tools and resources and configuration ports.
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.
IA-9	Multifactor authentication system established for critical areas.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high risk locations.
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.
SI: System and Information Integrity	
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.
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.
SI-3	Interactive system for managing password implemented to ensure password strength.
SI-4	Organization-wide clock synchronization system in place.
SI-5	Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as IT audit tools that can modify or delete audit data.

Table 3-2 (cont.)
Cybersecurity Controls

SC: System and Communications Protection	
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.
SC-2	Centralized authentication system or single sign-on established to authorize access 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.
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.
SC-5	Anomaly based IDS/IPS established including policies and procedures.
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.
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.
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.
SC-9	Process isolation established to provide a manual override “air gap” between highly sensitive systems and regular environments.
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).
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).
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.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.
AT: Awareness and Training	
AT-1	A security awareness and response program established to ensure staff is aware of security policies and incident response/notification procedures.
AT-2	Security training including Incident response training for employees, contractors and third party users based on job roles.
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.
PL: Planning ***CP: Contingency Planning*** ***IR: Incident Response***	
IR-1	Incident response program established to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events.
IR-2	A security program established 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.
IR-3	A legal/contractual/regulatory framework established 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.

3.4 Referenced Standards

To provide the user with more detailed information on the steps necessary to implement the recommended cybersecurity controls, specific references to existing NIST, AWWA, and 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 3.3 provides a list of the referenced standards.

Table 3-3
List of Standards & Guidance

	Name	Overview
DHS-CAT	U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers	A body of recommended practices across industries and agencies to prevent cyber-attacks.
DHS DID	DHS Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies	A body of recommended practices specific to ICS and emphasizing Defense in Depth Strategies.
NIST 800-82	National Institute of Standards and Technology (NIST) SP800-82 Guide to Industrial Control Systems (ICS) Security	The canonical standard for ICS systems.
NIST 800-53	NIST SP800-53 Rev. 3 with Appendix I Recommended Security Controls for Federal Information Systems and Organizations	A comprehensive framework of controls to be used to create complex security controls and monitoring systems.
NIST 800-34	NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems	Instructions and recommendations to implement short term recovery of damaged systems after an attack.
NIST 800-124	NIST Special Publication 800-124r1 Guidelines for Managing the Security of Mobile Devices in the Enterprise	Considerations and guidelines for the implementation of mobile systems
ANSI/AWWA G430-09	Security Practices for Operations and Management	Considerations and guidelines for the implementation of action for security of PCS systems.
*ANSI/AWWA G440-11	Emergency Preparedness Practices	Considerations and guidelines for the implementation of action for security of PCS systems.
*ANSI/AWWA J100-10	Risk and Resilience Management for Water and Wastewater Systems	Considerations of response and recovery actions that may include cyber-attack scenario.
*WRF/EPA/AWWA	Business Continuity Planning for Water Utilities	Considerations of disaster response plan for critical business enterprise systems including IT and PCS.
ISA-62443	ISA-99: Industrial Automation and Control Systems Security, ANSI/ISA 99	Considerations and guidelines for the implementation of PCS systems
ISO/IEC 27K	ISO/IEC 27000-27007 + 15408: Information technology - Security techniques - Code of practice for information security management (formerly ISO/IEC 17799:2000)	A certifiable framework to implement security programs.

* These standards are included in the cross reference to the NIST Framework (Appendix A).

Appendix A: Cross Reference to NIST 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 February 12, 2014.

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

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY – cont'd	Governance	ID.GV-1	Organizational information security policy is established	IR-2
		ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PS-2
		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
	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
		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

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT	Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users	IA-1
		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
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	IA-3
		PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	SC-8, SC-9
	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
		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

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*	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
		PR.IP-10	Response and recovery plans are tested	PS-4
		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

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*	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
		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

Function	Category	Sub-Category	Description	AWWA Guidance Control
DETECT – cont'd	Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability adequate awareness of anomalous events.	PS-2
		DE.DP-2	Detection activities comply with all applicable requirements	IR-3
		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, WRF/EPA/AWWA
		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, WRF/EPA/AWWA
		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

Function	Category	Sub-Category	Description	AWWA Guidance Control
RESPOND – cont'd	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, WRF/EPA/AWWA
		RS.IM-2	Response strategies are updated	ANSI/AWWA G430, G440, WRF/EPA/AWWA
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, WRF/EPA/AWWA
		RC.IM-2	Recovery strategies are updated	ANSI/AWWA G430, G440, WRF/EPA/AWWA
	Communications	RC.CO-1	Public relations are managed	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RC.CO-2	Reputation after an event is repaired	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	ANSI/AWWA G430, G440, WRF/EPA/AWWA

NOTES

American Water Works Association

Dedicated to the World's Most Important Resource™

Government Affairs Office
1300 Eye St. NW, Suite 701W
Washington, DC 20005
T: 202.628.8303
F: 202.628.2846