Which cybersecurity standard is most relevant for a water utility?

Don Dickinson[1]*

[1]Don Dickinson, Phoenix Contact USA, 586 Fulling Mill Road, Middletown, Pennsylvania, USA, 17057 (*correspondence: ddickinson@phoenixcon.com; 800-888-7388, ext. 3868)

KEYWORDS
ANSI/ISA-99 (62443), AWWA Cybersecurity Guidance & Tool, Cybersecurity, Cyber Security Management System (CSMS), Department of Homeland Security (DHS), Industrial Automation and Control Systems (IACS), Industrial Control System (ICS), International Society of Automation (ISA), National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework, Process Control System (PCS), Supervisory Control and Data Acquisition (SCADA)

ABSTRACT
Presidential Executive Order 13636 (EO) – *Improving Critical Infrastructure Cybersecurity* was issued February 2013.[1] The EO directed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework strengthening the resilience of critical infrastructure and protecting the national and economic security of the US. The NIST Cybersecurity Framework Version 1.0 (Framework) was released in February 2014 as required by the EO. The Framework relies on "existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk." [2]

Concurrent with the development of the Framework, the American Water Works Association (AWWA) initiated development of cybersecurity guidance to "provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber-attacks." [3] The AWWA Process Control System Security Guidance for the Water Sector and web-based Cybersecurity Tool (Guidance for both) were released in February 2014 as well.

The NIST Framework and AWWA Guidance are important resources for enhancing the security and resiliency of critical infrastructure. Both reference the various cybersecurity standards currently available. But which cybersecurity standard is the most relevant for a water utility?

One of the key standards referenced in both the NIST Framework and AWWA Guidance is ANSI/ISA-99, now known as ISA-62443. The multipart standard for industrial automation and control system security was developed by the International Society of Automation (ISA) and provides a flexible framework for developing a comprehensive security plan for utilities, including the establishment of policies and procedures essential to a cybersecurity management system.

The paper and presentation, *Which cybersecurity standard is most relevant for a water utility?* will provide an overview of the NIST Framework and the AWWA Guidance, how ISA-62443 relates to both, and how ISA-62443 provides a standards-based approach for the development of a comprehensive security plan for a water utility.

INTRODUCTION
Although a minor point both the terms "cyber security" and "cybersecurity" are correct and used extensively. Because "cybersecurity" is used in the more recent government documents it will be used for the purposes of this paper except when referencing documents that use "cyber security" specifically.

The first step in developing a comprehensive security plan is identifying appropriate guidance to direct the process. The good news is that there is a lot of cybersecurity guidance. The bad news is that there may be too much! In a report to congress in 2011 the Government Accountability Office (GAO) reported that cybersecurity guidance is available for critical infrastructure sectors, including water, but that more can be done to promote its use. The

report also stated, "*Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture."* [4] The challenge of identifying the appropriate guidance is greater for those sectors, such as water and wastewater (W/WW), where there are no mandatory requirements for cybersecurity. Lacking clear direction on security requirements W/WW asset owners and operators must determine which cybersecurity standards are the most appropriate for their organizations.

The NIST Framework and AWWA Guidance are valuable resources because they both identify the most relevant security standards available for guidance. Regardless of which standards are referenced it is important to remember that protecting water and wastewater systems from cyber-attack is just one facet of a much larger conversation – protecting critical infrastructure.

PROTECTING CRITICAL INFRASTRUCTURE

Presidential Policy Directive – *Critical Infrastructure Security and Resilience* (PPD-21) advances a national policy via the Department of Homeland Security (DHS) to "*strengthen and maintain secure, functioning, and resilient critical infrastructure that includes assets, networks, and systems*." [5] PPD-21 identifies 16 critical infrastructure sectors, including the Water and Wastewater Systems Sector that must be secure, and able to withstand and rapidly recover from *all hazards* including cyber-attacks. These critical infrastructures are vital to public confidence and the Nation's safety, prosperity, and well-being.

A key component in protecting critical infrastructure is protecting the control and supervisory control and data acquisition (SCADA) systems used to monitor and control plant processes from cyber-events, both intended and unintended. This need is evidenced by the issuance in February 2013 of the Presidential Executive Order (EO-13636) – *Improving Critical Infrastructure Cybersecurity* [6] that directs the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework to reduce risk to critical infrastructure. The framework is intended to provide critical infrastructure owners and operators a flexible and repeatable approach to meeting baseline cybersecurity measures and controls. DHS and sector-specific agencies have begun creating voluntary programs to assist owners and operators of critical infrastructure in adopting the framework and adapting it to the unique environments of their sector. A preliminary version of the cybersecurity framework was released late 2013 for public review and comment. The final version of the framework was released in February 2014.

NIST CYBERSECURITY FRAMEWORK VERSION 1.0

The NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (Framework) was issued February 12, 2014. A companion Roadmap outlines NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration to increase its value to users. The Framework and Roadmap are available as a download from the NIST Framework web site (*www.nist.gov/cyberframework*).

The Framework is a voluntary, risk-based approach for managing cybersecurity risks for critical infrastructure. It references industry standards and best practices to help organizations manage cybersecurity risks. The Framework is not meant to replace an existing program but can be used as the foundation for a new cybersecurity program or as a means to improve an existing program.

The Framework consists of three parts:

- Framework Core
- Framework Implementation Tiers
- Framework Profile

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references common across all critical infrastructure sectors that are segmented into five functions. These functions organize basic cybersecurity activities at their highest level. The five functions are: *Identify, Protect, Detect, Respond, and Recover*. Each function is broken down into *Categories* that define groups of cybersecurity outcomes. The

Categories are further divided into *Subcategories* that define specific outcomes of technical and/or management activities. Each subcategory is then matched to Information References such as standards, guidelines and best practices. The Information Resources listed in the Framework represent the most frequently referenced cross-sector guidance at the time of the Framework's development. There may be newer, sector-specific guidance that is not listed as an Information Resource. One example is the AWWA Guidance previously referenced and discussed later in this paper.

The Framework Implementation Tiers characterize the organization's risk management practices as defined by one of four tiers with Tier 1 having the least amount of risk management and Tier 4 the highest. Each organization must determine which tier is appropriate for them to work towards given the organization's unique goals, feasibility of implementation, and acceptable level of cybersecurity risk. A brief description of each tier follows.

- Tier 1: *Partial* – Cybersecurity risk management practices are not formalized; limited awareness of cybersecurity risk at organizational level; cybersecurity risk is managed in an ad hoc manner
- Tier 2: *Risk Informed* – Risk management practices are approved by management but not established as policy throughout the organization; informal prioritization of cybersecurity activities; risk-informed, management-approved processes and procedures in place, and staff has adequate resources to perform cybersecurity duties
- Tier 3: *Repeatable* – Risk management practices are formally approved and expressed as policy; organizational practices are regularly updated as needed to meet business/mission requirements and a changing threat and technology landscape; risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed; personnel possess knowledge and skills to perform roles
- Tier 4: *Adaptive* – Organization adapts cybersecurity practices through a process of continuous improvement incorporating advanced cybersecurity technologies and practices; organization-wide approach to managing cybersecurity risk using risk-informed policies, processes, and procedures; cybersecurity risk management is part of the organizational culture

The Framework Profile helps an organization define a roadmap for moving from a "current" profile that defines current risk management practices, to a "desired" profile that defines the outcomes needed to achieve the desired cybersecurity risk management goals. A comparison of the current profile and the desired profile provides a gap analysis that can be used to establish a plan defining actions required to meet organizational goals, and prioritization of activities to ensure cost-effective allocation of resources.

The Framework addresses the broad security needs of all critical infrastructure sectors including the Water & Wastewater Systems sector; however, as noted in the Framework, it is not industry-specific. Sector-specific guidance is intended to aid in the adoption of the Framework while providing guidance that is directed to the unique requirements of that sector. AWWA has developed cybersecurity guidance to meet the unique needs of the Water and Wastewater Systems sector.

AWWA CYBERSECURITY GUIDANCE & TOOL

Concurrent with the development of the NIST Framework the American Water Works Association (AWWA) initiated the development of cybersecurity guidance that would specifically address the requirements of protecting process control systems (PCS) used by water utility owners and operators to control water processes. The goal was to provide guidance that would be both practical and actionable. The final versions of the AWWA Cybersecurity Guidance & Tool were released in February 2014. 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 (WSCC)." [7]

The AWWA Guidance consists of two parts; a document titled Process Control System Security Guidance for the Water Sector [8], and a web-based Cybersecurity Tool. [9] Both can be accessed at the AWWA web site (*www.awwa.org/cybersecurity*). The document is a free download. The Cybersecurity Tool requires a login to

access. Registering a login username and password is free and you do not have to be a member of AWWA to register for access.

The Process Control System Security Guidance for the Water Sector (PCS Guidance) document outlines key cybersecurity practices and controls that are the basis for the Cybersecurity Tool. The cybersecurity practices are a set of recommendations for improving PCS security for water utilities. These practices are intended to be practical and actionable while establishing the foundation for a more comprehensive security plan. The practices that were defined by subject matter experts identify important facets of cybersecurity and are segmented into the following areas:

Governance and Risk Management	*Telecommunications, Network Security, and Architecture*
Business Continuity and Disaster Recovery	*Physical Security of PCS Equipment*
Server and Workstation Hardening	*Service Level Agreements*
Access Control	*Operations Security*
Application Security	*Education*
Encryption	*Personnel Security*

Table 1: PCS Guidance Cybersecurity Practices

The recommended practices are further defined by a set of 82 cybersecurity controls that provide more detailed measures for implementing the recommended practices. The Cybersecurity Tool was developed to simplify implementation of the cybersecurity controls by directly linking each control to one of the referenced security standards. Which controls are relevant to a user is determined by the use case scenarios selected in the Cybersecurity Tool.

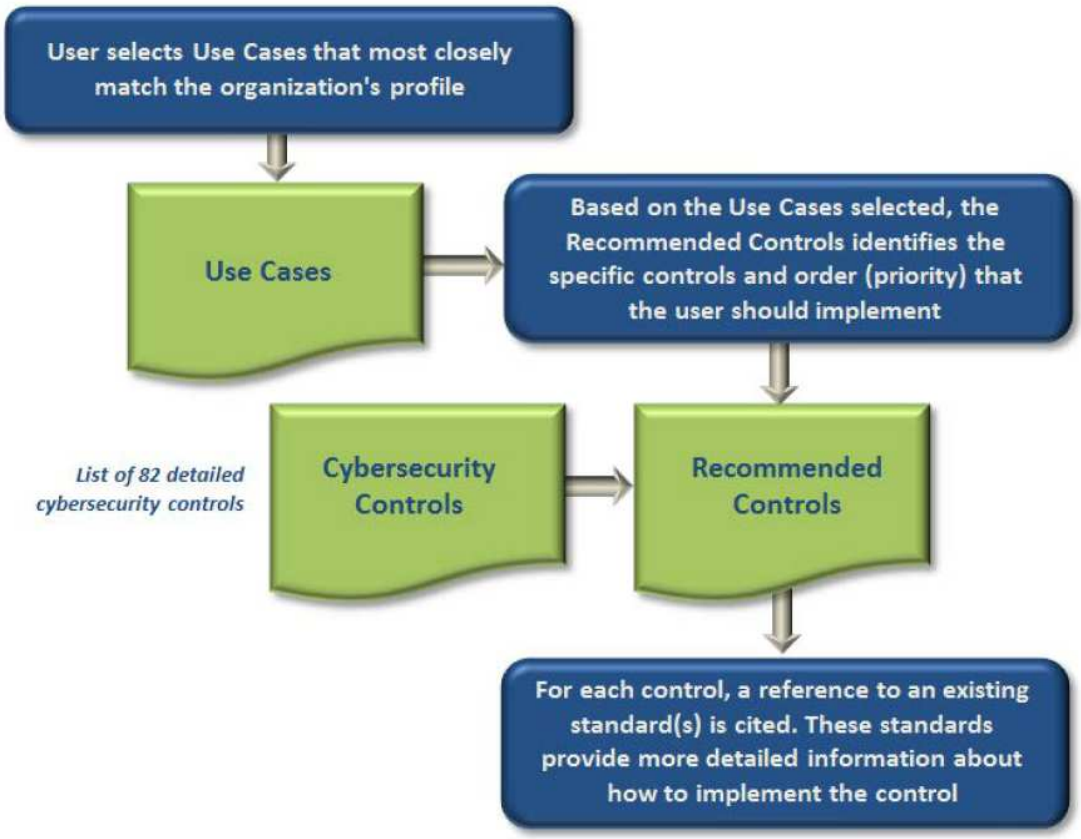

Figure 1: Cybersecurity Guidance Tool

A use case characterizes the manner in which a utility has designed and configured their PCS, and the connections between the PCS and external sources. Each use case represents a different type and degree of cybersecurity risk. The Guidance Tool determines the appropriate controls and priorities based on the various use case scenarios selected by the user. Once the applicable controls are determined the Guidance Tool identifies the specific section of the relevant standard that the user can reference for more detailed information. Figure 1 illustrates the process employed by the Cybersecurity Tool to link the various use case scenarios to specific standards.

Both the NIST Cybersecurity Framework and the AWWA Cyber Guidance reference the various cybersecurity standards that provide guidance to critical infrastructure sectors. As a result, owners and operators of W/WW operations now have a clearer understanding of the available cybersecurity standards and which may be the most relevant for their organization.

DEVELOPING A COMPREHENSIVE SECURITY PLAN

When developing a security plan to protect critical control and SCADA systems, it is important to remember that cybersecurity is not an absolute. It is not a "safe" verses "unsafe" matter. Security is a matter of degree. Additionally, because of limits to resources such as funding and personnel, it is neither practical nor feasible to mitigate all threats. There will always be risks associated with any plan. Asset owners and operators must determine acceptable levels of risk and establish an appropriate plan to mitigate known vulnerabilities. Further, because control systems and networks change over time, utilities must reassess risks and vulnerabilities on a recurring basis and security plans revised as needed.

Because there are no specific directives for securing industrial control systems in the W/WW sector the NIST Framework and AWWA Guidance are useful resources that identify relevant standards for cybersecurity. It is important to remember that the various standards are not mutually exclusive but complement one another. One standard is likely to provide more detailed guidance than another on a particular aspect of cybersecurity. As a result, all relevant security standards should be considered when developing and refining a security plan. However, it is the opinion of this writer that the ANSI/ISA-99 (62443) standard is the most relevant cybersecurity standard for developing a comprehensive security plan for a water utility.

ISA99 (62443) Security for Industrial Automation and Control Systems

The Industrial Automation and Control Systems Security committee (ISA99) of the International Society of Automation (ISA) produces "standards, recommended practices, technical reports and related information defining procedures for implementing electronically secure manufacturing and control systems, and security practices for assessing electronic security performance." [10] ISA-99 is a multipart standard for industrial automation and control systems (IACS) security. The ISA-99 standard provides guidance for a wide range of entities including those who design, implement or managing control systems as well as users, system integrators, security practitioners and, control systems manufacturers and vendors. The purpose of the standard is to "improve the confidentiality, integrity and availability of components or systems used for manufacturing or control, and provides criteria for procuring and implementing secure control systems." [11]

Originally all work products of the committee (standards, technical reports, etc.) were designated ISA-99.xx.yy, and this terminology is still in common use. More recently, after the ISA99 committee's work was adopted by the International Electrotechnical Commission (IEC) there was a decision to more closely align the ISA efforts with those of the corresponding IEC technical committee responsible for delivering a series of international standards designated as IEC 62443-x-y. As part of the plan to harmonize the numbering of ISA and IEC standards, the ISA work products are being renumbered from ISA-99.xx.yy to ISA-62443-x-y. The new designations will appear as each document is released or re-released.

Table 2 lists the key work products that have been released as standards. More detailed information about the ISA99 committee's work products is available at the ISA web site (*www.isa.org*).

Area of Focus	Target Audience	Designation	Title: Security for Industrial Automation and Control Systems:
General	All	ANSI/ISA-62443-1-1 (99.01.01) - 2007	Terminology, Concepts and Models
Policies and Procedures	Asset Owners	ANSI/ISA-62443-2-1 (99.02.01) - 2009	Establishing an Industrial Automation and Control System Security Program
System	System Integrators, Asset Owners, Product Suppliers, Service Providers	ANSI/ISA-62443-3-3 (99.03.03) - 2013	System Security Requirements and Security Levels

Table 2: Key ISA99 Committee Work Products Currently Available

ISA99 work products are intended for a wide range of audiences involved with the management, design, implementation or manufacturing of IACS. As noted in Table 2 the ISA99 work products each have an area of focus and intended audience. There are more work products in each category that are available, under development or planned. Additionally, there is a fourth area of focus, *Components* with work products under development. Work products in the *Components* category will address technical requirements for the development of secure IACS products. Manufacturers of IACS products and solutions are the primary target audience for these work products; however, asset owners and system integrators can benefit from these work products when specifying and procuring IACS products and solutions.

ANSI/ISA-62443-1-1 (99.01.01) - 2007 Terminology, Concepts and Models [12]

This standard describes the basic concepts and models relating to cybersecurity and serves as the basis for the ISA-62443 series. It focuses primarily on industrial automation, and control and SCADA systems used in critical infrastructure industries such as W/WW. In addition to defining key concepts and terminology the standard provides a series of models that can be used in the design of a security program. These control and SCADA system models are used to identify security needs at a level of detail necessary to address security issues with a common understanding of the framework and vocabulary.

ANSI/ISA-62443-2-1 (99.02.01) - 2009 Establishing an Industrial Automation and Control System Security Program [13]

As note previously, the target audiences for this standard are asset owners and operators responsible for establishing and managing a cybersecurity program for IACS. This standard describes the elements contained in a cyber-security management system (CSMS) for use in the IACS environment and provides guidance on how to develop those elements. These elements are primarily related to policy, procedures, practice and personnel and are grouped into three main categories:

- Risk analysis
- Addressing risk with the CSMS
- Monitoring and improving the CSMS

As noted in the standard, "It is not the intent of the standard to specify a particular sequential process for identifying and addressing risk that incorporates these elements. Thus, an organization will create such a process in accordance with its culture, organization, and the current status of its cyber security activities." [14] However, to assist organizations with application of the standard an example of a process for identifying and addressing risk is provided as well as a step-by-step guide that an organization can reference as they can begin to establish a CSMS.

Cyber Security Management System		
Risk analysis		
Business Rational		**Risk identification, classification and assessment**
Addressing risk with the CSMS		
Security policy, organization and awareness	**Selected security countermeasures**	**Implementation**
CSMS scope	*Personnel security*	*Risk management and implementation*
Organize for security	*Physical and environmental security*	*System development and maintenance*
Staff training and security awareness	*Network segmentation*	*Information and document management*
Business continuity plan	*Access control: Account administration*	*Incident planning and response*
Security policies and procedures	*Access control: Authentication*	
	Access control: Authorization	
Monitoring and improving the CSMS		
Conformance		**Review, improve and maintain the CSMS**

Table 3: Elements of a Cyber Security Management System

Risk analysis

The first main category of the CSMS is Risk Analysis that includes the business rational for establishing a security plan, and the means for assessing and managing risk. The business rational is based on the potential impact that a cyber-event can have on public health and safety, the environment, business continuity, emergency preparedness, and public confidence. The business rational may be the most important step in establishing a comprehensive security plan. Establishing a business rational is essential for an organization to maintain management buy-in at an appropriate level of investment for the IACS cyber security program.

Once there is a well-defined business rational that has the support of management the process of establishing a CSMS can begin. That process begins with assessing risk and defining how to mitigate risk to an acceptable level that is practical and cost-effective. There are numerous risk assessment methodologies available on the market that identify and prioritize risks related to IACS assets. A free Cyber Security Evaluation Tool (CSET) available from DHS is discussed later in this paper.

Addressing risk with the CSMS
The second main category is addressing risk with a CSMS. This category contains the bulk of the CSMS requirements and is divided into three element groups:

- Security policy, organization and awareness
- Selected security countermeasures
- Implementation

A review of the elements provides an indication that *cybersecurity is more about people than technology*. An effective cybersecurity program demands that an organization clearly define roles and responsibilities for implementing the program, establish clear and enforceable security policies and procedures, build awareness of the need for security throughout the organization, and provide training for support personnel. After there is a clear commitment to IACS security, risk assessed, and policies and procedures in place, effective countermeasures can be implemented to raise the organization's IACS security profile.

The CSMS outlines select security countermeasures that are fundamental to a well-designed security plan. The standard does not provide direction on how to fully implement these countermeasures but does discuss many of the policy, procedural, and practice issues relating to these particular countermeasures. There are additional countermeasures an organization will want to consider and integrate into the CSMS as the result of their risk assessment. The ISA-62443-3-3 standard, System Security Requirements and Security Levels provides more detail on these and other countermeasures that an organization may consider to address its unique cybersecurity requirements. Another standard to reference for guidance on cybersecurity countermeasures is NIST 800-82 Guide to Industrial Control Systems (ICS) Security (June 2011). [15]

The third element group in this category is Implementation and discusses issues relating to implementing the CSMS. A key component of this category is Incident Planning and Response that directs the organization to predefine how to detect and react to cybersecurity events. Good planning in this area can greatly reduce the impact of a cyber-event and enhance resilience.

The third main category is Monitoring and improving the CSMS. Elements in this category ensure that the CSMS is being used and its effectiveness reviewed on a regular basis.

ANSI/ISA-62443-3-3 (99.03.03) - 2013 System Security Requirements and Security Levels
The latest ISA99 work product to be released as a standard is ANSI/ISA-62443-3-3-2013 (August 2013).[16] The standard complements the other ISA-62443 work products by providing more detailed guidance on technical requirements for IACS security. The standard is useful in evaluating system design, and the suitability of products and services in meeting the asset owner's target control system security levels.

Assessing risk
When developing a security plan to protect critical control and SCADA systems, it is important to remember that cybersecurity is not an absolute. It is not a "safe" verses "unsafe" matter. Security is a matter of degree. Additionally, because of limits to resources such as funding and personnel, it is neither practical nor feasible to mitigate all threats. There will always be risks associated with any plan. Asset owners and operators must determine acceptable levels of risk and establish an appropriate plan to mitigate known vulnerabilities. Further, because control systems and networks change over time, utilities must reassess risks and vulnerabilities on a recurring basis and security plans revised as needed.

Developing an actionable plan for protecting critical systems begins with understanding vulnerabilities and associated mitigation strategies. There are a variety of assessment tools available to aid in this process.
Risk is defined as a function of the likelihood of an event, vulnerability to the event, and the consequence of the event. Risk assessment methodologies assess the general security posture of a utility and are instrumental in

helping asset owners and operators make informed decisions on resource allocation to mitigate risk in the most efficient manner possible.

CSET

Risk assessment tools are available to aid in the evaluation of IACS security. A useful tool from DHS is the Cyber Security Evaluation Tool (CSET®) [17] that assists organizations in protecting their key cyber assets. CSET is a stand-alone, desktop software tool that guides users through a step-by-step process to assess their control system and IT network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems. CSET is available from the DHS National Cyber Security Division as a free download.

AWWA J100-10 Risk and Resilience Management of Water and Wastewater Systems

Cyber risk assessment tools such as CSET are useful in securing critical control systems and thus help to protect critical infrastructure. However, asset owners may want a more holistic security methodology, one that mitigates risk for *all hazards*, both naturally occurring and intended attacks. As noted previously, a key directive of PPD-21 Critical Infrastructure Security and Resilience, "Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards." [18]

The AWWA J100-10 standard, Risk and Resilience Management of Water and Wastewater Systems [19] meets that need. J100-10 is a process for analyzing and managing the risks to water and wastewater systems associated with intended attacks, such as a cyber-attack, and naturally occurring hazards such as hurricanes and tornadoes. As part of a J100-10 analysis, risks from specific reference threat scenarios can be quantified to assess options for reducing these elements of risk. This process allows for evaluation of the benefit (changes in threat likelihood, vulnerability, and/or consequences) versus the cost of a specific countermeasures or mitigation option. As a result, decisions on resource allocation can be made based on the benefit-to-cost ratio ensuring the most efficient use of resources to protect critical assets.

One of the J100-10 reference hazards is Sabotage, either by physical attack or a cyber-attack. In both scenarios the attack can be quantified as an attack by an insider or by someone outside the organization. By including cyber-attacks as a reference hazard, J100-10 ensures that all hazards are considered when developing a security plan.

SUMMARY

Presidential Executive Order 13636 – *Improving Critical Infrastructure Cybersecurity* recognizes that the cyber threat to critical infrastructure, including the Water and Wastewater Systems sector, continues to grow and represents one of the most serious national security challenges for the United States. A comprehensive cybersecurity plan is fundamental to ensuring the future availability and reliability of water and wastewater systems. There is a wide range of cyber guidance available for asset owners and operators as referenced by the NIST Framework and AWWA Guidance including the ISA-62443 standard for Industrial Automation and Control Systems Security. ISA-62443 provides guidance for the establishment of a cybersecurity management system and may be the most relevant standard for the W/WW sector. Additionally, the AWWA J-100 Risk and Resilience Management of Water and Wastewater Systems standard provides a methodology to assess and manage risks from *all hazards*.

LIST OF ACRONYMS

AWWA	American Water Works Association
CSET	Cyber Security Evaluation Tool
CSMS	Cyber Security Management System
DHS	Department of Homeland Security
EO	Executive Order
GAO	Government Accountability Office
IEC	International Electrotechnical Commission
ISA	International Society of Automation
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System(s)
NIST	National Institute of Standards and Technology
PCS	Process Control System(s)
PPD	Presidential Policy Directive
SCADA	Supervisory Control and Data Acquisition
WSCC	Water Sector Coordinating Council
W/WW	Water/Wastewater

REFERENCES

[1, 6] Executive Order – Improving Critical Infrastructure Cybersecurity. February 12, 2013. Web. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. February 12, 2014. Web. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[3, 7, 8] American Water Works Association. Process Control System Security Guidance for the Water Sector. 2014. Web. http://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf

[4] U.S. Government Accountability Office. GAO-12-92. CRITICAL INFRASTRUCTURE PROTECTION, Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. December 2011.

[5, 18] Presidential Policy Directive (PPD-21) – Critical Infrastructure Security and Resilience. February 12, 2013. Web. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[9] American Water Works Association. Cybersecurity Tool. Web. http://www.awwa.org/resources-tools/water-utility-management/cybersecurity-guidance.aspx

[10, 11] International Society of Automation. ISA99, Industrial Automation and Control Systems Security. Web. https://www.isa.org/isa99/

[12] ANSI/ISA-99.01.01-2007: Security for Industrial Automation and Control Systems, Part -1: Terminology, Concepts, and Models. October 2007.

[13, 14] ANSI/ISA-99.02.01-2009: Security for Industrial Automation and Control Systems, Part -2: Establishing an Industrial Automation and Control System Security Program. August 2013.

[15] National Institute of Standards and Technology. NIST 800-82 Guide to Industrial Control Systems (ICS) Security. June 2011.

[16] ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for Industrial Automation and Control Systems, Part 3-3: System Security Requirements and Security Levels. August 2013.

[17] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cyber Security Evaluation Tool (CSET®). Web. http://ics-cert.us-cert.gov/Assessments

[19] ANSI/AWWA J100-10 Risk and Resilience Management of Water and Wastewater Systems (RAMCAP). July 2010.

About the Author:

Don Dickinson has 30 years of sales, marketing and product application experience in Industrial Controls and Automation, involving a wide range of products and technologies in various industry segments. Don is the Senior Business Development Manager – Water Sector, Phoenix Contact USA. He is the past chair of the NC AWWA-WEA Automation Committee and the current chair of the Automation Security subcommittee.