American Water Works Association

The Authoritative Resource on Safe Water℠

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005-3314
***T** 202.628.8303*
***F** 202.628.2846*

Advocacy
Communications
Conferences
Education and Training
Science and Technology
Sections

February 23, 2016

Via e-mail to cyberframework@nist.gov

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899

Re: AWWA comments in response to NIST's Solicitation for Comments on 'Views on the Framework for Improving Critical Infrastructure Cybersecurity'

The American Water Works Association (AWWA) appreciates the opportunity to respond to the National Institute of Standards and Technology (NIST) Solicitation for Comments on the Views on the Framework for Improving Critical Infrastructure Cybersecurity noticed on December 11, 2015. AWWA has been an active participant in the development of the Cybersecurity Framework ('Framework'). We also were one of the first organizations to provide a voluntary, sector-specific approach for implementing the Framework based on a use-case approach that allows the users to prioritize the controls measures applicable to a given function(s).

AWWA's response is specifically focused on questions associated with use of the Framework. We have attempted to provide a substantive and helpful response to these the questions. In terms of the remaining questions regarding updates to the Framework, we recommend that the NIST work with sectors to continue building awareness and providing resource to enhance the capacity for implementing various controls as part of a robust cybersecurity risk management program.

Use of the Framework:

1. Describe your organization and its interest in the Framework.

The American Water Works Association (AWWA) is an international, nonprofit, scientific and educational society dedicated to the improvement of drinking water quality and supply. Founded in 1881, AWWA is the largest organization of water supply professionals in the world. Our membership represents the full spectrum of the drinking water community: treatment plant operators and managers, environmental advocates, engineers, scientists, academicians, and others who hold a genuine interest in water supply and public health. Our membership includes more than 4,500 utilities that supply roughly 80 percent of the nation's drinking water.

AWWA is an American National Standards Institute (ANSI) accredited standards development organization (SDO), and the only SDO in the water sector. These comments are in part intended to remind NIST of the value provided by voluntary consensus based standards, such as those developed by AWWA under the ANSI framework. The "private sector" is often the most efficient

means to address various issues in the marketplace that require a common baseline, which in the case of the water includes business enterprise and process control systems. In fact, since the organizations founding in 1881, AWWA has developed 196 consensus standards and 52 manuals of practice to promote clean, safe water. One of the key purposes of the association, as stated in original charter, is "for the exchange of information pertaining to the management of water-works, for the mutual advancement of consumers and water companies, and for the purpose of securing economy and uniformity in the operations of water-works."

AWWA standards represent over 100 years of development of water-service practice under the direction of AWWA by volunteer committee members, including producers, consumers, and general interest groups. Over the years, AWWA has developed rules and procedures that provide for the inception, checking, rechecking, and final establishment of standards that define the minimum requirements for materials, products, systems, and services with respect to good water-service practices. All of this work is performed to protect the general public and to continue the improvement of the water-supply field, which now include standards that support the security and resiliency of the water sector.

Given our mission, AWWA recognizes the value and intent of Executive Order 13636: *Improving Critical Infrastructure Cybersecurity* and welcomes the opportunity to make NIST aware of a suite of standards and associated manuals/guidance, described below, that have been developed by AWWA that complement the objectives in the Executive Order and the Framework.

AWWA Resources

Roadmap to Secure Control Systems in the Water Sector

This project was developed in 2008 by AWWA in collaboration with the Department of homeland Security National Cyber Security Division, and endorsed by the Water Sector Coordination. The roadmap—combined with other initiatives— aims to provide a framework to address the full range of needs for mitigating cyber security risk of industrial control systems (ICS) across the water sector. For this roadmap, ICS are defined as the facilities, systems, equipment, services, and diagnostics that provide the functional control and/or monitoring capabilities necessary for the effective and reliable operation of the water sector infrastructure. While recognizing the importance of physical protection, this roadmap focuses on the cyber security of ICS. It does not specifically address the security of other business or cyber systems, except as they interface directly with the water sector ICS. This roadmap covers goals, milestones, and activities over the near (0-1 year), mid (1-3 years), and long term (3-10 years). Security activities encompass recommended practices, outreach, training, certifications, software patches, next-generation technologies, change management, information exchange, and implementation.

Process Control System Security Guidance for the Water Sector and supporting Use-Case Tool

Based on recommendations in the 2008 Roadmap to Secure Industrial Control Systems in the Water Sector, AWWA's Water Utility Council took action to develop a cybersecurity resource designed to provide actionable information for utility owner/operators based on their use of process control systems. That is the purpose and objective of the Process Control System Security Guidance for the

Water Sector and the supporting Use-Case Tool. This resource has been recognized by the Water Sector Coordinating Council and the USEPA as the foundation of a voluntary, sector-specific approach for adopting the Framework.

All in all, this requires a commitment to action as part of an all-hazards risk management strategy as recommended in ANSI/AWWA G430: Security Practices for Operations and Management. The AWWA Cybersecurity Guidance & Tool are living documents, and it is expected that further revisions and enhancements will be implemented based on input from users (update pending for early 2016).

ANSI/AWWA G430-14: Security Practices for Operations and Management

The purpose of this standard is to define the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety, and public confidence. This standard is one of several in our Utility Management series, designed to cover the principal activities of a typical water and/or wastewater utility. This AWWA standard has received SAFETY Act designation from the Department of Homeland Security.

This standard is intended to apply to all water or wastewater utilities, regardless of size, location, ownership, or regulatory status. This standard builds on the long-standing practice amongst utilities of utilizing a multiple barrier approach for the protection of public health and safety. The requirements of this standard are designed to support a protective utility-specific security program that will result in consistent and measurable outcomes that address the full spectrum of risk management from organizational commitment, physical and cyber security, and emergency preparedness. As an example, the standard includes the following requirement which is specific to cyber security:

> ***4.8.2 Protecting IT, Process Control Systems, and SCADA systems****. The utility should review the AWWA Process Control System Security Guidance for the Water Sector as an aid in evaluating appropriate practices and controls for securing Process Control System and/or SCADA vulnerabilities. These strategies may also be useful in securing critical business IT systems for the business continuity plan.*
>
> ***4.8.2.1 Restricting access.*** *The utility shall identify and implement steps necessary to control access to critical IT and SCADA systems to only authorized persons conducting official utility business. Physical hardening and procedural controls shall be considered and implemented. Examples of procedural controls include:*
>
> - *Restricting access to data networks,*
> - *Safeguarding critical data through backups and storage in safe places,*
> - *Establishing procedures to restrict network access,*
> - *Implementing policies to ensure that IT contractors or their products will not negatively affect IT systems.*

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

This standard provides a consistent and technically sound methodology to identify, analyze, quantify, and communicate the risks of specific terrorist attacks and natural hazards against critical water and wastewater systems, and establishes requirements for the risk and resilience assessment and management process that inform decisions on allocation of resources to reduce risk and enhance resilience through countermeasures and mitigation strategies. The standard documents a process for identifying security vulnerabilities and provides methods to evaluate the options for improving these weaknesses. This AWWA standard has received SAFETY Act designation from the Department of Homeland Security.

The threat of cyber intrusion is one of several required reference threats, based on Department of Homeland Security guidance, which a utility must include when completing an assessment. The J100 methodology allows the utility to incorporate the consequences from the impairment of business enterprise or process control into the risk assessment. It is recommended that a utility leverage resources such as the Cyber Security Evaluation Tool (CSET) available from DHS to assist them in this analysis. In fact, CSET is an outgrowth of a water sector research project managed by the Water Environment Research Foundation under a grant from the USEPA.

ANSI/AWWA G440-11: Emergency Preparedness Practices

This standard defines the minimum requirements for emergency preparedness for a water or wastewater utility and expands upon the requirements outlined in G430. Emergency preparedness practices include the development of an emergency response plan (hazard evaluation, hazard mitigation, response planning, and mutual aid agreements), the evaluation of the emergency response plan through exercises, and the revision of the emergency response plan after exercises. This standard is one of several in our Utility Management series designed to cover the principal activities of a typical water and/or wastewater utility.

This standard is supplemented by ***Manual 19 (M19): Emergency Planning for Water Utilities***. M19 was first issued in 1973 to provide guidelines and procedures that can be used by utilities of any size. Revisions of the manual are in progress to reflect current the state of knowledge regarding emergency preparedness and the G440 standard.

These resources are complemented by ***Business Continuity Plans for Water Utilities***, which is a joint effort led by the Water Research Foundation, AWWA and USEPA. The genesis for developing this resource was the recognition that utilities needed sector specific guidance as recommended by the Water Sector Coordination Council. This resource provides a template to support utility development of a BCP, which includes a Disaster Response Plan (DRP). The DRP is a plan that addresses response and recovery for the Information Technology (IT) component of the organization, including by not limited to the following:

- Clearly established IT system security, mitigation, response and recovery policies
- Redundancy of critical systems, components and capabilities

- Interoperability between system components and between the primary and alternate locations
- Annual review and testing of plans capturing technological changes

Manual 2 (M2): Instrumentation and Control

This manual was first developed in 1968 and is currently under revision. The manual is written primarily to support water utility operations staff in understanding the principles of electrical systems, automation and instrumentation control that are found in water distribution, treatment and storage systems. The next edition, current under review, will include an expanded chapter on cybersecurity.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

AWWA was one an early supporter of the Framework. AWWA is a user of the Framework in the context that we have developed resources that enable water systems to easily evaluate the controls that may apply to their operation needs. In collaboration with our sector specific agency, the US Environmental Protection Agency, and the Water Sector Coordinating Council we have promoted the Framework through various platforms, but most specific via usage of the AWWA Use-Case tool.

3. If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).

AWWA has actually developed a use-case approach to supporting the water sectors application of the Framework. The AWWA guidance and tool is designed to provide water utility managers with a consistent approach that maps directly to Framework which enables them to easily assess what control measures may be necessary to support an effective cyber risk management strategy. Water utilities have reported using the AWWA Use-Case Tool in the following manner:

1. As a stand-alone tool to identify an appropriate cybersecurity baseline. When used as a stand-alone effort, the tool:
    - Allows non-technical users to identify cybersecurity controls and practices applicable to a utility of their size and complexity.
    - References cybersecurity standards applicable to the drinking water and wastewater utility SCADA/PCS environment.
    - Provides a “target baseline” for securing the system appropriately.

    In this context the AWWA Use-Case Tool is applied in two modes, depending on the user’s perspective:
    - In a “top down” mode, the tool can be used by management to ask meaningful questions of their technical staff to identify if and how recommended practices are followed, and to prioritize efforts based on gaps, shortcomings and the need for additional assistance.
    - In a “bottom up” mode, the tool can be used by support personnel to demonstrate a need for cybersecurity improvements to management. Citing a “higher authority”

(standards and best practices) lends credence to requests for equipment, services and training. Identifying gaps highlights areas where additional skills and training are needed.

2. As part of a larger cybersecurity assessment to validate findings and recommendations. Under this scenario, the tool provides additional value and validation of findings:
    - Running the tool at the end of an assessment allows Use Cases to be more accurately identified.
    - Assessment results can be correlated against assessment findings.
    - Priorities can be modified based on unique conditions.
    - Correlating findings and recommendations to best practices and standards that support the business case.

3. As the basis for a cybersecurity improvements program. Under this scenario, the tool can be used as the basis for a Cybersecurity Improvements Program, providing a basis for development of cybersecurity policy and practices:
    - The tool is recognized as the water sector approach to applying the Framework in response to EO13636.
    - The tool identifies a target baseline for cyber security.
    - The cited standards can be used to build the business case for specification of more robust products and services.

4. What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?

AWWA members have reported a positive experience with the flexible nature provided by AWWA's Use-Case approach for examining the controls defined in Framework that are relevant to their operational conditions. AWWA's prioritization of control also provide utility managers with a reason approach to implementing controls in a systematic manner that can be reasonable accommodated in budgeting cycles as appropriate.

5. What portions of the Framework are most useful?

The Core Functions and Categories provided the baseline for development of AWWA's Use-Case approach and these are generally consistent with our existing risk management practices easing the alignment of language and implementation in our use cases.

6. What portions of the Framework are least useful?

In working with water sector utilities and subject matter experts, we found the Tiering process to be the least valuable aspect of the Framework. While we understand the conceptual purpose, the diversity within the sector renders this approach almost meaningless since the operational conditions of each systems are so diverse. We essentially found this to be distraction from our primary objective of making cybersecurity more accessible to utility managers in a manner that did not require in-depth technical expertise.

7. **Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?**

   As noted in a 2014 Water Sector Cybersecurity CIPAC report, awareness remains a key limiting factor. This is partially due to the fact that much of the information provided to critical infrastructure owners/operators is strictly focused on threats with very limited discussion of probability and consequence. For managers in any sector that may not have in-depth technical knowledge of how such threats might impact an organization this absence of knowledge challenges the business case, especially in a constrained budget environment.

8. **To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.**

   AWWA does not collect any specific data on the security actions of water utilities. However, we are developing multiple case studies on utilities that have applied the AWWA Use-Case tool to create or supplement their cyber security risk management program.