American Water Works Association
The Authoritative Resource on Safe Water SM

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005
T 202.628.8303
F 202.628.2846
www.awwa.org

Headquarters Office
6666 W. Quincy Avenue
Denver CO 80235
T 303.794.7711
F 303.347.0804

October 10, 2014

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

RE: Experience with the Framework for Improving Critical Infrastructure Cybersecurity (79 FR 50891)

Dear Ms. Honeycutt:

Enclosed are the comments of the American Water Works Association (AWWA) in response to the request for information issued by the National Institute of Standards and Technology (NIST) on August 26, 2014 (79 FR 50891). AWWA appreciates the opportunity to comment and we look forward to collaborating with NIST to ensure that the resources developed to address this issue are of the greatest utility to critical infrastructure owners and operators in the water sector.

If you have any questions about these comments, please feel free to contact me or Kevin Morley in our Washington Office.

Yours Sincerely,

Thomas W. Curtis
Deputy Executive Director

Comments of the American Water Works Association

Experience with the Framework for Improving Critical Infrastructure Cybersecurity (79 FR 50891)

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.

AWWA recognizes the value and intent of Executive Order 13636: Improving Critical Infrastructure Cybersecurity and welcomes the opportunity to offer these comments for consideration as NIST proceeds with actions that support implementation of the cybersecurity framework. AWWA has taken several steps to integrate cybersecurity into our suite of standards and associated manuals/guidance which collectively support the voluntary adoption of the NIST Cybersecurity Framework (CSF).

Current Awareness of the Cybersecurity Framework

1. *What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?*

   AWWA is participating in Cybersecurity Awareness Month and has included cybersecurity awareness messages in our monthly periodicals, which have a readership surpassing 102,000. We are in the process of releasing additional promotional materials to elevate awareness of cybersecurity and the resources we have developed to support utilities, see response to Question 3.

2. *How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?*

   See response to Question 1 & 3.

3. *Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?*

On February 12, 2014, AWWA released a resource entitled ***Process Control System Security Guidance for the Water Sector and Use-Case Tool (www.awwa.org/cybersecruity)*** to provide a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems. The target audiences for this resource are water utility General Managers, Chief Information Officers and Directors with oversight and responsibility for process control systems. This guidance has been recognized by the Water Sector Coordinating Council as the foundation of a sector-specific approach to voluntary adoption of the NIST CSF. In addition, the US Environmental Protection Agency stated in May 2014 letter to White House regarding EO 13636, that the

In 2008, the *Roadmap to Secure Control Systems in the Water Sector* identified a series of challenges and gaps related to advancing the cyber security protocols of the sector. Recent assessments have supported pronouncements that the number one threat to the Nation's critical infrastructure is a cyber-attack. This was in part the stimulus for Executive Order 13636: Improving Critical Infrastructure Cybersecurity. At a minimum, AWWA believes that the release of the water sector guidance and tool will support voluntary adoption of the NIST CSF. The AWWA guidance was specifically designed to align with the NIST CSF, but applies a slightly different "framework" to enhance use by utility managers that may not be as familiar with the detailed control protocols for cybersecurity in the NIST CSF.

AWWA's use-case approach presents the issue from the perspective of how the utility applies a suite of technologies to support various operational objectives (e.g. remotely operate a pump station with control). Based on the use-case selected, a prioritized list of controls is generated that represent optimal conditions that can be used by the utility to compare with current operational conditions. The prioritization is based on peer-review by subject matter experts familiar with water sector process control systems. This use-case approach breaks the issue of cybersecurity down into an operational relevant format that utility manager find more approachable and contextual to their working conditions. The prioritization makes the issue less daunting since a utility with limited resources can focus on priority 1 control's that will generate immediate vulnerability reductions and proceed accordingly. All of the controls in the AWWA guidance are mapped directly to the NIST CSF.

The control domains included the AWWA guidance and reports generated by the use-case tool empower utility owners with the information needed to engage the issue internally with staff and/or externally with service providers. It also provided a valuable baseline set of best practices that elevate the expectations placed on prospective service providers that support

many small and medium size utilities, while giving assurance that it supports national homeland security objectives outlined in the NIST CSF and EO 13636.

This resource has been distributed for free, presented at AWWA's annual conference and multiple section conferences, webinars, the WaterISAC, the ISC-ISAC and other venues. It will also be featured prominently during the AWWA Water Infrastructure Conference in Atlanta, October 26-28.

4. *Is there general awareness that the Framework:*
   a. *Is intended for voluntary use?*
   b. *Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?*

      Yes, this has been communicated consistently with the sector both in reference to the NIST CSF directly and it is embedded into the AWWA guidance and use-case tool. This also aligns with the voluntary consensus standards that AWWA has issued for the water sector covering security and preparedness.

   c. *Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?*

      Yes, we support the approach taken by NIST to leverage existing voluntary consensus standards consistent with the National Technology Transfer and Advancement Act of 1995 and OMB Circular A-119.

5. *What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?*

   Helping to contextualize the risk management outcomes associated with implementing the various controls outlined in the NIST CSF. Perhaps more important is developing some basic cybersecurity training and educational resources for non-technical decision makers. In essence not everyone needs to become cybersecurity technician, but management needs to understand the basic taxonomy and principles so they can engage the subject and understand the value of implementing various controls practices.

6. *Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?*

   AWWA has members around the world and the resources we provide are available to members and non-members alike.

7. *If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?*

   The US Environmental Protection Agency (EPA) has been an active partner in elevating the awareness of the water sector about the importance of cybersecurity. They contributed to the development of the AWWA guidance and use-case tool to ensure alignment with the principles in the NIST CSF. In response to the mandated review of existing authorities by federal agencies, EPA's response to the White House included the following statement:

   > ….the American Water Works Association has issued "Process Control System Security Guidance for the Water Sector" and a supporting "Use-Case Tool." This guidance identifies prioritized actions to reduce cybersecurity risk at a water or wastewater facility. The cybersecurity actions are aligned with the Cybersecurity Framework. **This tool is serving as implementation guidance for the Cybersecurity Framework in the Water and Wastewater Systems sector.**

8. *Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?*

   See response to Question 1 & 3.

9. *What more can and should be done to raise awareness?*

   We encourage NIST and the DHS C-Cubed program to reference the AWWA guidance and use-case tool since they are complimentary to the NIST CSF as recognized by our SCC and sector-specific agency. Current Framework and C-Cubed outreach materials do not acknowledge the proactive steps the water sector has taken to enhance cybersecurity, which can lead to confusion about what a water utility should be doing. This is especially discouraging since EO 13636 supports the development of sector-specific guidance, yet repeated attempts to have the AWWA resources integrated or referenced by NIST and DHS appear to be ignored.

   Give the experience of NIST and ICS-CERT, critical infrastructure sectors would benefit from additional information that contextualizes the consequences to better communicate the impacts and/or benefits of various control strategies. In addition, there is very limited data that supports a simple understanding of the threat from a probabilistic perspective such that an owner can make informed risk management decisions for resource allocations under

constrained budget conditions. For example, a modeling approach[1] that facilitates risk assessment of common cyber-attack scenarios with likely probabilities of successful attack for each scenario that could be generally applicable to many sectors.

Experiences with the Cybersecurity Framework

Given that the NIST Framework and corresponding AWWA guidance and use-case tool have only been deployed for ~7 months we believe that experience will grow with time. We are at an early stage of awareness and therefore specific experiences have not been fully captured. In addition, certain control practices require significant planning and capital investment to ensure appropriate implementation and assurances to maintain operational continuity.

Anecdotally, AWWA has observed an increase in technical presentations at national and regional conferences in content that covers cybersecurity case studies by utilities and support contractors. This serves to both raise general awareness and provide peer examples of how similar systems have enhanced their cybersecurity protocols. In addition, we are encouraged by the cumulative web traffic associated with the AWWA guidance and use-case tool, over 4,000 individual users, since it was released.

In addition, the Water Sector Coordinating Council and Government Coordinating Council have convened the CIPAC Water Sector Cybersecurity Strategy Workgroup to promote and facilitate use of the Cybersecurity Framework. This workgroup is preparing recommendations on approaches for outreach and training that will promote use of the NIST CSF and build capacity by all segments of the sector, leveraging AWWA's guidance and use case tool as a baseline.

In addition to the resources referenced above AWWA has a full suite of resources that integrate cybersecurity into the risk management practices applied by the water sector as described below:

1. *Roadmap to Secure Control Systems in the Water Sector*
   The *Roadmap* was developed in 2008 by AWWA in collaboration with the Department of Homeland Security, National Cyber Security Division, and endorsed by the Water Sector Coordinating Council. 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

[1] Dudorov, Stupples & Newby (2013). Probability analysis of cyber attack paths against business and commercial enterprise systems. 2013 European Intelligence and Security Informatics Conference. DOI 10.1109/EISIC.2013.13

sector infrastructure. While recognizing the importance of physical protection, the *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. Security activities encompass recommended practices, outreach, training, certifications, software patches, next-generation technologies, change management, information exchange, and implementation.

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

The G430 standard defines 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 received SAFETY Act designation from the Department of Homeland Security in February 2012.

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 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, this standard includes several requirements that address cyber security, including the following:

> 4.8.1 Define security-sensitive systems and information. For most systems, information technology (IT), Process Control Systems, and SCADA systems are essential to the efficient and continuous operations of a utility. The utility shall identify critical IT, Process Control Systems, or SCADA systems as security sensitive. The utility shall also identify other security-sensitive information. This information review shall consider facility maps and other geographic sources on utility operations, security plans, vulnerability assessments, or other technical details that could aid an adversary in the planning or execution of an attack. For additional information and useful tools for critical cyber system identification and protection, the user is directed to appendix A, Section A.7—AWWA Process Control System Security Guidance for the Water Sector, and Section A.8—Cyber Security Evaluation Tool (CSET).

3. ***ANSI/AWWA J100-10: Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems***

   The J100 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. The standard 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 received SAFETY Act designation from the Department of Homeland Security in February 2012.

   The threat of a cyber-attack is one of several required reference threats, base on Department of Homeland Security guidance, which a utility must include when completing a J100 assessment. The J100 methodology allows the utility to incorporate the consequences from the impairment of business enterprise or process control systems 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.

4. ***ANSI/AWWA G440-11: Emergency Preparedness Practices***

   The G440 standard defines the minimum requirements for emergency preparedness for a water or wastewater utility and expands upon 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 also 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 Coordinating 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 but 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

5. ***Manual 2 (M2): Instrumentation and Control***

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