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

April 8, 2013

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

(via *cyberframework@nist.gov*)

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity (78 FR 13034)

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 February 26, 2013 (78 FR 13034). AWWA appreciates the opportunity to comment and we have several items we believed should be considered by NIST as it proceeds with the development of the cybersecurity framework. 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,

Tom Curtis

Thomas W. Curtis
Deputy Executive Director

Comments of the American Water Works Association

Developing a Framework to Improve Critical Infrastructure Cybersecurity (78 FR 13034)

Overview

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 manual of practice to promote clean, safe water. One of the key purposes of the association, as stated in our 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 in water-service practices 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 requirements for materials, products, systems, and services with respect to 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 includes standards that support the security and resiliency of the water sector.

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 development of the cybersecurity framework. Specifically, AWWA would like to make NIST aware of a suite of standards and associated manuals/guidance, described below, that have been developed or planned by AWWA that we believe address or support the actions defined in the Executive Order.

Current Activity

Process Control System Security Guidance for the Water Sector

The purpose of this project is to develop water sector guidance that provides a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems. The target audience for this resource are water utility General Managers, Chief Information Officers and Utility Directors with oversight and responsibility for process control systems.

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. More recently, Executive Order 13636: Improving Critical Infrastructure Cybersecurity was issued to strengthen the cybersecurity of critical infrastructure by increasing information sharing and developing a framework of cybersecurity practices, which is the subject of the NIST request for information. At a minimum, AWWA believes that the development of this guidance will inform the NIST process and represent the water sector's approach to support the Cybersecurity Framework based on collaboration with key partners and stakeholders. We believe that this resource will act a critical bridge between the highly technical resources that have been develop by NIST and others, and the principles we expect to be defined in the Cybersecurity Framework.

Existing Resources

1. *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 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 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 G430-09: 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:

> ***4.8.2.1 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.*

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 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

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.