ASSOCIATION OF METROPOLITAN WATER AGENCIES

LEADERS IN WATER

1620 I Street, NW, Suite 500
Washington, DC 20006

P 202.331.2820
amwa.net

December 19, 2022

Via water_nccoe@nist.gov

Re: Comments on *Securing Water and Wastewater Utilities: Cybersecurity for the Water and Wastewater Systems Sector*

To Whom It May Concern:

The Association of Metropolitan Water Agencies (AMWA) appreciates the opportunity to provide these comments in response to the draft project description, *Securing Water and Wastewater Utilities: Cybersecurity for the Water and Wastewater Systems Sector*, published by the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST).

As an organization representing the largest publicly owned drinking water systems in the United States, whose members generally serve more than 100,000 people, we recognize the importance of providing resources to help water utility managers build awareness of cybersecurity threats and improve their cybersecurity posture. We appreciate that the goal of the practice guide is to provide illustrative cases that demonstrate solutions using commercially available products and services for a given set of scenario-based challenges. However, we are interested to learn how this finished product will compare with the existing relevant standards and guidance available to the water sector (listed in Section 4 of the draft document). We also encourage NCCoE to make explicitly clear that the document does not propose the establishment of any cybersecurity standards or practices that would be binding upon drinking water or wastewater systems; instead, there must be a clear understanding that the practice guide is only intended to serve as a resource to help identify practical steps that water systems can voluntarily take to address cyber challenges.

With that in mind, several of our members have offered the following feedback, clarifications, suggestions, and additions to specific components of the draft document:

- Lines 83-84: NCCoE should be clearer in defining the universe of water utilities that are envisioned as part of the target audience of this practice guide. While the Executive Summary reports that the project's focus "is on municipal-scale utilities," the Safe Drinking Water Act defines a "community water system" as a public water system that "regularly serves at least 25 year-round residents." Furthermore, according to EPA data, more than half of the roughly 50,000 community water systems across the country serve populations of 500 people or fewer. Therefore, the nation's range of "municipal-scale" drinking water systems is extremely large,

and includes many systems that face widely varying threat profiles and response capabilities. To the extent that the practice guide is targeted at more or less sophisticated water systems, that should be made clear and also acknowledge that there also many other community water systems that may require different cyber-related assistance.

- Line 161: Industrial Control System Manufactures do not allow installation of management tools or agents on the devices allowing IT best practices to enhance the management of the OT environment.

- Lines 170 and 180: Backups are important, but it is unclear how this may fit under an Asset Management scenario or solution.

- Line 182: Legacy and current ICS protocols (such as Modbus/TCP, ICCP, etc.) are clear text and do not require authentication. Transitioning and existing system to DNP3 is a significant upgrade and not all ICS devices support modern protocols. Furthermore, most utilities cannot afford to make this transition.

- Lines 191 and 199: Testing is important, but it is unclear how this may fit under the topic of Data Integrity.

- Line 201: Multifactor authentication should be required for all privileged access within critical infrastructure. If manufactures are unable to build this into their systems, then municipalities should be encouraged to provide the multifactor authentication technology and functionality.

- Line 202: The sentence states, "Threat actors can obtain access to the network through many avenues, such as credential harvesting, phishing campaigns, or access to cleartext identification and authentication data." This is unclear. If the bad actor can access cleartext ID and authentication data, it seems that they would already be on the network. One potential rephrasing of the sentence could read as, "Threat actors can obtain access to the network through many avenues, such as credential harvesting **or** phishing campaigns, **resulting in ~~or~~** access to cleartext identification and authentication data."

- Line 251: Wireless Communication for control is a risk, because we cannot prevent jamming of RF signals. If wireless is unavailable, municipalities must be able to manually operate their systems.

- Line 338: The Security Control Map would be more effective if the target audience was the water and wastewater control system provider (i.e., product manufacturers), rather than the water and wastewater asset owners. In that case, an asset owner could create an RFP for manufacturers that specifies that a product must be consistent with the NIST Security Control Map. Additionally, the controls could be renamed "Baseline Security Controls for Water & Wastewater Control System Manufactures" to provide it with greater stature and name recognition among stakeholders.

Beyond the scenarios and recommendations laid out in the draft document, additional cyber-related threats may warrant inclusion in the project guide. For example, insider threats (where an employee with authorized access to a control system attempts to cause damage), are not referenced in the document. It would therefore be worthwhile for the guide to reference this scenario and offer utilities guidance on how to minimize the risks posed by individuals with access to the system.

Again, AMWA appreciates the opportunity to provide feedback on the draft project description, *Securing Water and Wastewater Utilities: Cybersecurity for the Water and Wastewater Systems Sector*. We believe this has the potential to serve as a guide to help drinking water and wastewater systems evaluate and mitigate identified cybersecurity risks, and we look forward to reviewing the final product.

Sincerely

Tom Dobbins
Chief Executive Officer