American Water Works Association

Dedicated to the World's Most Important Resource®

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

January 19, 2018

Submitted via E-Mail to cyberframework@nist.gov

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

RE: AWWA response to NIST's Solicitation for Comments on "Cybersecurity Framework Version 1.1 Draft 2"

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 Cybersecurity Framework Version 1.1, Draft 2. AWWA has been actively promoting use of the Cybersecurity Framework ('Framework') since it was first issued in 2014. We 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 control measures applicable to a given function(s).

We commend NIST for the collaborative process used to develop and refine the Framework with stakeholders. The revisions outlined in Draft 2 reflect our interest in maintaining flexibility in how the Framework is applied to support an entity's cybersecurity risk management needs. The clarification that the Framework is intended to be a resource for self-assessment aligns well with the AWWA resources that have been developed to provide a tailored review of applicable controls for various use-cases. The addition of supply chain controls is appropriate, but would note the absence of reference to NIST SP 800-191 in the Framework Core. AWWA will work to incorporate these updates into our resources once finalized by NIST.

AWWA, an awardee of the 2016 NIPP Resilience Challenge, has launch a national initiative to promote the use of the Framework in the water sector based the resources we have developed. Given this experience, we do find the Tiering process to be the least valuable aspect of the Framework. While the conceptual purpose is understandable, it tends to be a distraction from the primary objective of making these essential cybersecurity risk management practices more accessible, and in a format that supports continued monitoring by utility managers. As noted in prior comments, AWWA's use-case tool generates a prioritized list of controls that supports self-assessment and risk management. This self-assessment approach allows the user to "right-size" the controls for any given system function being reviewed.

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

Yours Sincerely,

G. Tracy Mehan, III

G. Tracy Mehan, III
Executive Director – Government Affair