Water Environment Federation
the water quality people™

601 Wythe Street, Alexandria, Virginia 22314-1994 | p 703.684.2400 | f 703.684.2492 | www.wef.org

April 8, 2013

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

Re: ''Developing a Framework to Improve Critical Infrastructure Cybersecurity''

The Water Environment Federation (WEF)[1] appreciates the opportunity to comment on the National Institute of Standards and Technology (NIST) initiative in developing a framework to improve critical infrastructure cybersecurity.

In the United States, drinking water and wastewater utilities, collectively known as the Water Sector, are charged with implementing programs to provide water services for their communities everyday regardless of external forces, including natural disasters or malevolent events, that may impede their efforts. To provide their essential services, water sector utilities do not operate independently. In fact, the water sector is interdependent with every critical infrastructure. Therefore, the denial of drinking water and wastewater utilities' services—whether the result of a natural disaster, physical attack, or cyber attack—would have cascading effects.

Advanced preparation to plan to continually provide drinking water and wastewater services during and following an incident will reduce human and economic hardships. The water sector identified cyber attacks on instrumentation and control systems as one of five threat themes in its sector specific plan. Water sector utility sub-assets, or components, are classified as physical, cyber, and human. Physical components include water source (groundwater or surface water) for drinking water utilities and collection systems for wastewater utilities. Cyber components for both drinking water and wastewater facilities include control systems known as Supervisory Control and Data Acquisition (SCADA) systems. Human components consist of employees and contractors charged with managing and operating a utility. The water sector depends on the reliable functioning of critical infrastructure, which has become increasingly dependent on information technology.

Steps must be taken to enhance existing efforts to increase the protection and resilience of water sector infrastructure, including the maintenance of a cyber environment that encourages efficiency, innovation, and economic prosperity, while protecting privacy and civil liberties. Increased resilience is a major objective of all critical infrastructures, understanding and appreciating water sector interdependencies is essential to this process. To enhance existing guidance, the communication of voluntary, cost-effective, and non-burdensome cybersecurity practices for water and wastewater utilities of all sizes, as well as the development of corresponding training and education can encourage improved cybersecurity.

[1] / Founded in 1928, the Water Environment Federation (WEF) is a not-for-profit technical and educational organization of 36,000 individual members and 75 affiliated Member Associations representing water quality professionals around the world. WEF members, member associations, and staff proudly work to achieve our mission to provide bold leadership, champion innovation, connect water professionals, and leverage knowledge to support clean and safe water worldwide.

The Water Environment Federation looks forward to engaging in the development process as well as participating in discussions with other sector representatives to assist in meeting the NIST goals of Framework development.

Best regards,

Jeff Eger
Executive Director

As requested by NIST in FR notice (78 Fed. Reg. No. 38, Feb. 26, 2013, p 13024), these comments were submitted online to cyberframework@nist.gov.