

EXECUTIVE COMMITTEE
PRESIDENT

Suzanne E. Goss

Government Relations Specialist
JEA (Electric, Water & Sewer)
Jacksonville, FL

VICE PRESIDENT

Julius Ciaccia, Jr.

Executive Director
Northeast Ohio Regional
Sewer District
Cleveland, OH

TREASURER

Karen L. Pallansch

Chief Executive Officer
Alexandria Renew Enterprises
Alexandria, VA

SECRETARY

Adel H. Hagekhalil

Assistant Director
Bureau of Sanitation
City of Los Angeles
Los Angeles, CA

PAST PRESIDENT

David R. Williams

Director of Wastewater
East Bay Municipal
Utility District
Oakland, CA

EXECUTIVE DIRECTOR

Ken Kirk

April 8, 2013

Diane Honeycutt

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
Via Email: cyberframework@nist.gov

**Re: NACWA Comments on Request for Information, Developing a Framework
to Improve Critical Infrastructure Cybersecurity**

Dear Ms. Honeycutt:

The National Association of Clean Water Agencies (NACWA) appreciates this opportunity to comment on the National Institute of Standards and Technology's (NIST) request for information on developing a framework to improve critical infrastructure cybersecurity ("Framework"). NACWA represents the interests of nearly 300 publicly owned wastewater treatment agencies nationwide, serving the majority of the sewered population in the U.S. NACWA members range greatly in size, serving populations of less than 2,000 to more than eight million. NACWA is involved with improving the security, emergency preparedness, and resiliency of wastewater utilities through its active Security and Emergency Preparedness Committee and its work with the Water Sector Coordinating Council.

NACWA members have taken many voluntary steps to improve both the physical security of their systems and their cybersecurity. While NACWA recognizes that the Framework will not include regulations or mandates, the Association encourages NIST to consider the measures already taken voluntarily by utilities and the improvements that utilities will continue to make to their cybersecurity as risks are identified. Since publicly owned wastewater utilities are also facing tremendous costs to upgrade their existing infrastructure and to meet the regulatory requirements of the Clean Water Act, any recommendations contained in the Framework regarding cybersecurity improvements should be cost-effective and not overly burdensome to utilities.

The recommendations of the Framework, and any burden placed on utilities by these recommendations, should be proportional to the risks associated with a cybersecurity incident at a wastewater facility. The Cyber-Dependent Infrastructure Identification working group established by the Department of Homeland Security

has been charged with identifying the risks that a cybersecurity incident for critical infrastructure could have on public health or safety and economic or national security. The Framework should consider the relative risks from an incident at a wastewater utility, compared to other facilities, and reflect these risks in its recommendations.

NACWA also asks that NIST develop the Framework with enough flexibility to accommodate the variability in wastewater utility sizes, treatment processes, and management structures. Some wastewater utilities are part of a municipal or county government, while others are separate entities. Many utilities do not have their own information technology (IT) systems, but instead use services from another city or county department, and therefore the utility has limited control over these systems. The Framework should account for the various organizational structures for IT systems at utilities, recognizing that the cybersecurity expertise at some utilities may be limited, while other utilities may have their own personnel to implement improvements.

Most importantly, NIST should provide multiple opportunities for input from wastewater and drinking water utilities throughout the Framework development process, both from the water sector associations and from the Water Sector Coordinating Council. Allowing ample input will result in a Framework that provides effective and practical recommendations for improving cybersecurity at utilities.

Thank you for consideration of these comments. NACWA looks forward to providing more specific input on the Framework as it is developed. Please contact me at 202-533-1836 or cfinley@nacwa.org if you have any questions.

Sincerely,

A handwritten signature in cursive script that reads "Cynthia A. Finley".

Cynthia A. Finley
Director, Regulatory Affairs