January 31, 2024

The Honoroable Buddy Carter
Chairman
Subcommittee on Enivironment,
Manufacturing, & Critical Materials
Committee on Energy and Commerce
U.S. House of Represenatives
Washington, DC 20515

The Honorable Paul Tonko
Ranking Member
Subcomittee on Environment,
Manufacturing, & Critical Materials
Committee on Energy and Commerce
U.S. House of Representaitves
Washington, DC 20515

RE: Perspectives of Public Clean Water Agencies and Professionals on Ensuring the Cybersecurity of America's Water Sector Utilities

Dear Chairman Carter and Ranking Member Tonko,

On behalf of the National Association of Clean Water Agencies (NACWA) and the Water Environment Federation (WEF), we thank you for holding today's hearing of the House Energy & Commerce's Environment, Manufacturing, & Critical Materials Subcommittee on Ensuring the Cybersecurity of America's Drinking Water Systems.

NACWA represents public wastewater and stormwater agencies of all sizes nationwide, with more than 350 public agency members. WEF serves as the not-for-profit technical and educational organization of 35,000 individual members and 75 affiliated Member Associations representing water quality professionals worldwide.

While NACWA and WEF primarily work on clean water policy and advocacy issues, we understand that today's hearing – although mainly focused on drinking water issues – may touch on topics and potential regulatory approaches that would impact clean water utilities. Accordingly, we submit these comments to provide our perspective on these issues as they relate to public clean water utilities. Our comments are not intended to provide any opinion or position on cybersecurity issues as they apply to drinking water utilities.

Properly treated and managed wastewater and stormwater are essential in protecting both public health and the environment. With more than 16,000 publicly owned treatment works (POTWs) throughout the nation that treat more than 75 percent of America's wastewater, public clean water agencies play a prominent role in protecting the public by treating billions of gallons of the nation's wastewater. To ensure continuity of treatment while cyber threats continue to target America's critical infrastructure, efforts must be made to provide public utilities with robust voluntary resources to better protect themselves from cyberattacks.

Many utilities have taken proactive steps to improve their cybersecurity, investing their limited ratepayer funds to protect their infrastructure and operations. NACWA and WEF are very appreciative of the extensive resources that already exist at the federal level:

- The Cybersecurity and Infrastructure Security Agency (CISA) provides free vulnerability scanning services for utilities and resources, such as guidance on best practices, the Cyber Security Evaluation Tool, and vulnerability alerts and updates.
- The U.S. Environmental Protection Agency (EPA) provides free technical assistance and cybersecurity assessment resources.
- The National Institute of Standards and Technology (NIST) provides many best practice resources, including the NIST Cybersecurity Framework.

In addition to these resources, several water sector organizations have developed additional tools for utilities to better prepare against cyber threats:

- The Water Information Sharing and Analysis Center (WaterISAC), a non-profit organization comprised of water and wastewater utility managers and administrators, provides up-to-date alerts, information, and analysis specifically for the water sector and is managed by the Association of Metropolitan Water Agencies (AMWA).
- The American Water Works Association (AWWA) has developed a Cybersecurity Assessment Tool and Guidance, which assists water sector utility operators on how best to implement applicable cyber controls based on the NIST Cybersecurity Framework that can significantly reduce a utility's vulnerability to a cyberattack.

Congress can help support clean water agencies in their efforts to leverage existing resources and improve cybersecurity in a variety of ways, including:

- The Energy and Commerce Committee should act favorably on H.R.1367, the *Water System Threat Preparedness and Resilience Act of 2023*, to offset the cost of WaterISAC membership for eligible utilities and help water systems be more aware and prepared for cyberattacks.
- Congress can require wastewater utilities to conduct risk and resilience assessments, including cyber vulnerability assessments, like those required for drinking water utilities under America's Water Infrastructure Act (AWIA) of 2018, and provide funds for small- and medium-sized utilities to conduct these assessments.

In addition, federal agencies should be encouraged to work with utilities and water sector associations to improve cybersecurity in a variety of ways that include:

- EPA, CISA, and WaterISAC should work with the vendors and contractors supplying equipment to the clean water sector to ensure that their products and services are set up and maintained appropriately to ensure that they are secure, including communicating to and training utility staff on best practices.
- EPA and CISA should continue providing federal support to help prevent attacks through training, cybersecurity services, technical assessments, and pre-attack planning and continue providing an incident response to assist the sector in reducing the scale and duration of impacts if attacked. The agencies should consider collaborating with NACWA and WEF to develop additional guidance documents and resources to help clean water utilities understand and implement cybersecurity best practices.
- Speed, flexibility, and responsiveness are critical in the rapidly evolving world of cybersecurity. Encouraging public utilities to use existing tools, resources, and best practices will improve resilience to cyber-attacks faster than cumbersome regulatory structures enacted by federal agencies or a third-party entity.

Lastly, as many clean water utilities are already fully engaged in improving and maintaining existing cybersecurity protocols, NACWA and WEF firmly believe that allowing clean water utilities to improve their cybersecurity voluntarily, rather than implementing a direct or third-party quasi-regulatory system, is the best approach for wastewater utilities for a variety of reasons that include:

- Developing a regulatory approach for clean water utilities, such as third-party oversight within EPA, will take years, and a one-size-fits-all approach to cybersecurity will not provide for innovative, collaborative, cross-sector approaches for developing, designing, and implementing successful cybersecurity programs in the sector.
- Clean water utilities can leverage existing resources immediately rather than waiting to see what regulations are finalized to avoid taking measures that may be duplicative or not meet the requirements of potential regulations.
- Since clean water utilities may be part of city or county government that are already subject to state cybersecurity requirements, a voluntary approach to cybersecurity allows flexibility for utilities to develop cybersecurity approaches and practices that meet their needs and that can be developed in line with best practices from other brother/sister utilities and city/county departments.

NACWA and WEF thank the Subcommittee for the opportunity to submit comments. We look forward to working with your members on federal policies that maintain and provide clean water utilities with resources that will provide speed, flexibility, and responsiveness to adapt to cybersecurity threats.

Encouraging public utilities to use existing tools, resources, and best practices will improve resilience to cyberattacks.

If you have any questions, please have your staff contact Matt McKenna (mmckenna@nacwa.org) or Steve Dye (sdye@wef.org).

Sincerely,

Nathan Gardner-Andrews
Chief Advocacy & Policy Officer
National Association of Clean Water Agencies

Steve Dye
Senior Director, Government Affairs
Water Environment Federation