Improving Cybersecurity for Public Clean Water Agencies

Cybersecurity is an increasing concern for the public clean water agencies that protect public health and the environment by managing and treating billions of gallons of the nation's wastewater and stormwater. Many utilities have taken proactive steps to improve their cybersecurity, investing their limited ratepayer funds to protect their infrastructure and operations.

Although no impacts occurred to water treatment or distribution, a recent cyber-attack on a drinking water utility in Pennsylvania illustrated how cyber vulnerabilities still exist at some utilities. Cybersecurity must continue to be improved and implemented at all wastewater utilities, and the National Association of Clean Water Agencies (NACWA) and the Water Environment Federation (WEF) believe that this will be accomplished more quickly and thoroughly through voluntary measures rather than through complicated new legislation or by creating a new regulatory scheme.

Extensive resources already exist to help clean water agencies improve their cybersecurity, including:

- The Cybersecurity and Infrastructure Security Agency (CISA) provides free vulnerability scanning services for utilities, as well as 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 a plethora of best practice resources, including the NIST Cybersecurity Framework.
- The Water Information Sharing and Analysis Center (WaterISAC) provides up-to-date alerts, information, and analysis specifically for the water sector.

NACWA and WEF have encouraged their public utility members to take advantage of all these resources.

Improving and maintaining cybersecurity is an ongoing, continuous process. Many utilities are already fully engaged in this process. 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:

- Developing a regulatory approach, 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.
- 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 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.

Clean water agencies can be supported by Congress, federal agencies, and the water sector associations in their efforts to improve cybersecurity in a variety of ways:

- Congress should pass S.660/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 that include 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.
- EPA, CISA, and WaterISAC should work with the vendors and contractors that supply 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 of 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 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 utilities understand and implement cybersecurity best practices.

Speed, flexibility, and responsiveness are key 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.

Contact Information

Matthew McKenna
Director, Government Affairs
National Association of Clean Water Agencies (NACWA)
202-263-9533
mmckenna@nacwa.org

Steve Dye
Senior Director, Government Affairs
Water Environment Federation (WEF)
703-684-2400, ext. 7213
sdye@wef.org