BARNES & THORNBURG LLP

New Law Requires Drinking Water Systems To Develop Risk, Cybersecurity And Resilience Assessments

February 28, 2019 | | Environmental,Water

Jeffrey M. Peabody
Partner

RELATED PRACTICE AREAS

Data Security and Privacy
Environmental
Environmental Crimes and Investigations

The new America's Water Infrastructure Act (AWIA), which primarily focuses on certain water infrastructure projects being undertaken by the U.S. Army Corps of Engineers, also created a number of new requirements applicable to community water systems serving more than 3,300 people.

Among other things, community water systems are required under the AWIA to conduct and report on a comprehensive water system risk and resilience assessment. They must also develop an emergency response plan that addresses both physical and cybersecurity threats. The AWIA, which was signed into law in October 2018, also creates a grant program that will assist community water systems with improving their operational resilience.

Water System Risk and Resilience Assessments Required For Community Water Systems

The AWIA requires each community water system serving more than 3,300 people to conduct an assessment of the risks to, and resilience of, its system. This assessment must include an assessment of:

- The risk of the system from malevolent acts and natural hazards
- Resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment,

treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system

- The monitoring practices of the system
- The financial infrastructure of the system
- The use, storage, or handling of various chemicals by the system
- The operation and maintenance of the system

The AWIA goes on to state that the required assessment may also include an evaluation of capital and operational needs for risk and resilience management for the system. This provision is consistent with a growing focus on prioritization of needs and the use of objective metrics to “score” competing projects seeking external funding.

The AWIA also authorizes the U.S. Environmental Protection Agency to create a grant program, called the “Drinking Water Infrastructure Risk and Resilience Program,” under which the EPA may award grants for the purpose of increasing the resilience of community water systems.

The law requires that each community water system certify that they have conducted the required assessment by a date certain, depending on the population served by the water system. For systems serving a population of 100,000 or more, the certification shall be made prior to March 31, 2020. For systems serving 50,000 to 100,000 customers, the certification is due by Dec. 31, 2020 and for those water systems serving between 3,300 and 50,000 customers, the risk assessment certification is due no later than June 30, 2021.
Given the comprehensive nature of the required risk and resilience assessment, community water systems should consider taking steps now to meet these deadlines.

Emergency Response Plans Must Include Cybersecurity Considerations

The AWIA builds upon the risk and resilience assessment requirement by further requiring community water systems to prepare or revise, as necessary, an emergency response plan that incorporates the findings from the risk assessment. This emergency response plan is due no later than six months after completion of the risk assessment.

Notably, the emergency response plan “shall include…strategies and resources to improve the resilience of the system, including the physical and cybersecurity of the system.”

While cybersecurity threats have been steadily increasing for the water and wastewater industries, the AWIA will require community water systems to assess their cybersecurity vulnerabilities in a comprehensive fashion. The requirement to include cybersecurity in a system’s emergency response plan will also help drinking system operators prepare for the increasingly inevitable cybersecurity attacks they will face in the future.