Cybersecurity in the Water and Wastewater Sector

ASDWA is the professional association that serves the leaders (and their staff) of the 57 state and territorial drinking water programs. Formed in 1984 to address a growing need for state administrators to have national representation, ASDWA has become a respected voice for states with Congress, EPA, other Federal agencies, and professional organizations in the water sector. ASDWA's members have worked closely with EPA, the Sector Risk Management Agency (SRMA) for the water and wastewater sector, on a wide range of physical security and cybersecurity issues for the past 20-plus years.

Cybersecurity is a National Concern:

Despite the growing awareness of cybersecurity as an emerging threat, infrastructure continues to experience cyber-based attacks at an alarming frequency, including ransomware and exploits of Industrial Control System (ICS) vulnerabilities. With more sophisticated cyberattacks on critical infrastructure on the rise, taking the right approach to stem this threat is so important. Cybersecurity threats to critical infrastructure are a national concern, and that concern is growing.

EPA's Proposed Approach is Problematic:

EPA has proposed an approach that includes assessing the cybersecurity vulnerabilities of Public Water Systems (PWSs) as part of the Sanitary Survey program. As part of this program, state inspectors visit PWSs on a 3 to 5-year cycle to evaluate the system's capacity to deliver safe drinking water.

EPA's proposal would have these inspectors require systems to conduct cybersecurity assessments and then, on subsequent visits 3-5 years later, evaluate their implementation of corrective actions. State sanitary survey inspectors are experts at reviewing water sources, treatment, and operations. They are not appropriately skilled to evaluate cybersecurity at PWSs, nor should they serve on the frontlines of a national cyber defense response. Diverting inspectors to cyber security activities will also take resources away from the critical sanitary survey inspection functions that lead to identifying contamination pathways and other issues that water systems need to address to keep tap water safe.

Several significant concerns with this approach have not been fully addressed, **such as the lack of subject matter expertise, lack of a standard to measure against, protection of sensitive information, potential liability for the states, the low frequency of sanitary surveys compared to rapidly evolving cybersecurity threats, and the state staff burden for assessing and monitoring systems' cybersecurity activities.** Sanitary survey results are public record, particularly if a significant deficiency is discovered and a violation is issued. States are concerned about how to protect this information, including cybersecurity vulnerabilities, from public disclosure and targeting by bad actors, and the states' resources that might be needed to protect this sensitive information.

ASDWA has repeatedly communicated these concerns to EPA over the past 18 months:

- Cybersecurity in the Water Sector - ASDWA President's Letter, September 29, 2021
- Cybersecurity Dialogue with the States – ASDWA Letter, February 9, 2022
- ASDWA Letter to EPA on Cybersecurity Implementation Guidance – November 21, 2022

A Proposed Alternative:

EPA, CISA, and states should ensure that systems receive educational and informational resources to increase awareness and promote cyber hygiene. The approach should encourage systems to conduct a cyber vulnerability assessment that could, if needed, lead to taking corrective actions based on the assessment results. EPA, CISA, and states should support systems by providing technical and assistance resources to help them identify possible threats and take corrective actions as part of their routine operations, not every few years when sanitary surveys take place, but over time as resources permit.

Additionally, EPA should leverage existing authorities under SDWA section 1445 to review a sample of risk and resiliency assessments and emergency response plans required under AWIA to identify opportunities to enhance training and target support resources where appropriate to ensure the most significant impact.

For more information, contact Anthony DeRosa of ASDWA at aderosa@asdwa.org .