asdwa

Association of State
Drinking Water Administrators

March 26, 2024

Kaitlyn Petersen, Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Re: ASDWA's Responses for Questions for the Record for January 31, 2024 Cybersecurity Hearing

Dear Ms. Petersen:

The Association of State Drinking Water Administrators (ASDWA) appreciated the opportunity to testify at the January 31, 2024, hearing entitled "Ensuring the Cybersecurity of America's Drinking Water Systems". Improving cybersecurity across the water sector is critical for water and wastewater systems continuing to protect public health and the environment 24/7/365 in the face of increasing cybersecurity threats. ASDWA's members, i.e., the state and territorial primacy agencies, play a key role in the day-to-day oversight of water systems, and will have play a role to meet the common goal of improving cybersecurity across the water sector.

The hearing covered a wide range of issues and there was good dialogue between the witnesses and the members during the question-and-answer portion of the hearing. Additional questions for the record resulted from the hearing (below) and ASDWA's response to these questions are shown below in italics:

<u>Responses to The Honorable Earl L. "Buddy" Carter</u>

1. **The hearing made clear that EPA collaboration on cybersecurity efforts needs to be improved. The drinking water systems that testified with you each expressed support for some kind of a cybersecurity standards regime where their input was as important as EPA's when it came to both deciding and establishing actual Federal cybersecurity standards.**

   a. **Cybersecurity standards setting is not an authority that the Safe Drinking Water Act currently gives to EPA nor permits it to be federally delegated to the States under section 1413. What do you think the State regulator's role should be in the utilities' suggested Federal cybersecurity standards setting organization (e.g. Water Risk and Resilience Organization)?** ASDWA's Cybersecurity Workgroup has limited knowledge on the Water Risk and Resilience Organization (WRRO) based on one briefing. That briefing generated several significant questions about that potential organization that warrant additional discussions to make an informed judgement on the proposed WRRO. A meeting is in the process of being scheduled for further discussions. Questions on applicability, verification of corrective actions, enforcement, protection of sensitive information, long-term funding, etc., need to be answered before a vision of the primacy agencies' role can be developed. There are significant concerns with systems being required to be a member of a new organization and be required to pay for membership in that organization.

Additionally, primacy agencies' role between the WRRO and the water systems is currently unclear, and adding another new organization between the water systems and the primacy agencies has the possibility of creating confusion and coordination challenges.

b. **At least one of our witnesses talked about the difference between the system for addressing cybersecurity at electric utilities and the one proposed for the water sector. Like the drinking water sector, the electricity sector has both large utilities serving customers in urban areas and municipal and rural systems.**

   i. **What do you see as the plusses and minuses of using something like that-system to address cybersecurity in the drinking water sector?** As previously stated, several questions about that potential organization warrant additional discussions, and a meeting is in the process of being scheduled for further discussions. Questions on applicability, verification of corrective actions, enforcement, protection of sensitive information, long-term funding, etc., need to be answered before a series of pluses and minuses can be developed for this proposed approach. Additionally, the electricity sector is significantly different than the water sector. First, the electricity sector is smaller – more than an order of magnitude smaller with approximately 2,000 utilities versus over 50,000 community water systems, and over 15,000 publicly owned treatment works (POTWs). Second, of the over 50,000 CWSs, approximately 80% serve less than 3,300 people and likely do not have a full-time operator/employee. Finally, the electricity sector primarily consists of large, privately-owned companies, as opposed to approximately 80% of CWSs being municipally or publicly owned systems.

c. **How many states have cybersecurity standards for the water sector?** Zero, if the traditional definition of "standards" applies, i.e., something numerical or a narrative that systems must take compliance samples for and check the monitoring result with the standard, with oversight by the primacy agencies, and enforcement actions that would be taken to address continued violations. Cybersecurity standards for the water sector will likely not look like the traditional Maximum Contaminant Levels (MCLs) or Treatment Techniques (TTs) developed under the Safe Drinking Water Act (SDWA). A small number of primacy agencies have requirements to conduct cybersecurity assessments but no requirements for corrective actions. Another small group of primacy agencies have cybersecurity guidelines. The challenge for both the water and wastewater systems and primacy agencies is moving from guidelines and/or best practices to regulatory requirements that are feasible and enforceable across the sector.

d. **What role should state cybersecurity standards for the water sector play versus Federal ones, and who should get deference if there is conflict or overlap between them?** As previously stated, zero primacy agencies have cybersecurity standards and state deference should be continued for cybersecurity. Primacy agencies currently can be stricter than the Federal baseline. Primacy agencies have decades of experience with large and small systems and continually make small adjustments in their regulatory oversight to match what is seen in the field without compromising public health protection.

e. **What do you expect to be the resource demand on States if the Federal government regulates cybersecurity in the water sector?** New regulations for cybersecurity will require increased resources for primacy agencies. The extent of the increased demands is unknown until any potential regulatory requirements are proposed. The extent of those increased resource demands is currently unclear, but any increase is problematic given the converging regulatory burden of implementation of the increased funding from the Infrastructure Investment and Jobs Act (IIJA), the upcoming final regulation for per- and polyfluoroalkyl substances (PFAS), the Lead and Copper Rule Revisions (LCRR) and Lead and Copper Rule Improvements (LCRI), the revisions to the Consumer Confidence Report (CCR) Rule, and the traditional activities such as providing technical assistance, system inspections, review of construction plans and specifications, training and certification of operators, etc.

Responses to The Honorable Frank Pallone, Jr.

1. **Is it important that any cybersecurity framework include not only an assessment of risks, but also corrective actions to address identified deficiencies? What can federal agencies do to assist utilities in implementing necessary corrective actions?** Improving cybersecurity preparedness and response across the water sector will require both assessments and corrective actions by thousands of water and wastewater systems. If nothing is corrected with any of the "issues" identified in the assessment, then the status quo remains the same. Federal agencies, primarily EPA and CISA, will need to play key roles in these efforts, and that will require additional resources, i.e., Congress will need to appropriate additional funds to these agencies to assist water and water systems in a collaborative manner. Systems will need additional funding if significant capital improvements, e.g., replacement of all Programmable Logic Controllers (PLCs) throughout the system due to them being outdated, are needed.

Again, ASDWA appreciated the opportunity to testify at this hearing. If any additional information is needed on the challenging cybersecurity issues for the water sector, please feel free to reach out to me at aroberson@asdwa.org

Sincerely yours,

J. Alan Roberson

J. Alan Roberson, P.E.
Executive Director

Cathy Tucker-Vogel

Cathy Tucker-Vogel
Public Water Supply Section Chief
Bureau of Water
Kansas Dept. of Health and Environment

Cc: David Travers – EPA
Lauren Wisniewski - CISA