Kevin Morley, American Water Works Association
July 31, 2024

Response to Additional Questions for the Record from the January 31, 2024, hearing entitled "Ensuring the Cybersecurity of America's Drinking Water Systems."

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

1. Your testimony is supportive of creating a Water Risk and Resilience Organization (WRRO).
   a. Please state the merits of the WRRO process the American Water Works Association has recommended?
      - The governance model created by the WRRO approach provides the necessary federal oversight from the U.S. Environmental Protection Agency (EPA) while leveraging subject matter expertise from the field to develop appropriate cybersecurity requirements.
      - A one-size-fits-all set of requirements is simply not reasonable given the broad spectrum of technology applications used to support various functions across an array of system sizes. This level of diversity across systems requires a tiered risk and performance-based approach to setting requirements for drinking water and wastewater systems, which is best developed by subject matter experts.
      - The WRRO provides independent, third-party assessments of a water system's implementation of cybersecurity requirements in a manner that protects sensitive information. These assessments are beyond the technical capacity of states and EPA to perform effectively in a non-intrusive manner.
      - Findings from these assessments will aid utilities with credit ratings and insurance underwriting.
      - Reports on compliance will be provided to states and EPA annually.

   b. Why is there general support for the concept among other water utility associations?
      - There is general recognition that sector stakeholders should be directly involved in the development and management of cybersecurity requirements.

   c. Do you think there is confusion about the role EPA should play in the WRRO? If yes, please state what Environmental Protection Agency's role would be.
      - The governance model created by the WRRO approach provides the necessary federal oversight from EPA as the sector risk management agency. EPA would have final approval over cybersecurity requirements and any enforcement actions associated with failure to comply with those requirements.

2. What challenges do you see with the WRRO model being applied to the water sector for cybersecurity?
      - This approach has been effectively implemented in the electric sector, but it would represent the first public-private governance model applied to the water sector.
      - There will be a need to recognize existing compliance obligations that exist based on state or other federal requirements via a reciprocity type approach assuming equivalency.

3. You recently testified before the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection that the EPA should remain as the Sector Risk Management Agency for the Water and Wastewater sector. Do you believe that reorienting EPAs technical assistance program would provide greater efficiencies for addressing cybersecurity challenges in the sector?

   - We would like to see EPA work more directly with sector partners like AWWA that have trusted relationships at the state level. This provides a significant force multiplier in knowledge transfer that EPA cannot duplicate cost effectively with staff or contractors.
   - Multiple resources are available to assist systems of all sizes and this need is closely linked with training and education to ensure capacity is developed to leverage existing resources vs. developing new resources. It has been our experience that collaborating on training to demonstrate how existing tools and services, such as AWWA's cyber assessment tool, has been highly effective in enabling water utility staff to implement fundamental cybersecurity controls. For example, the Indiana Section of AWWA partnered with the State Infrastructure Development Bank to deliver multiple trainings across the state to several hundred water system owner/operators. This approach leverages trusted partners to deliver critical information in a workshop environment that also provides peer-to-peer knowledge sharing.

4. Even though EPA is the Federal expert on water and wastewater treatment and use in communities, Congress was careful to avoid giving regulatory authority to EPA in this space because it would hamstring the ability of the EPA and the sector to be flexible and resilient in responding to incidents.

   a. Both Safe Drinking Water Act section 1433 and the WRRO proposal are very different models for EPA. Does your experience suggest EPA is willing to voluntarily shift away from direct regulatory implementation?

      - It is our observation that across multiple programs EPA seems to be moving toward a greater level of direct regulatory implementation, including provisions with clear state primacy.
      - The WRRO model maintains EPA oversight function while addressing recognized capacity limits in terms of technical expertise and resources. In developing cyber requirements, the WRRO process leverages the knowledge of a wide array of stakeholders, including state and federal partners. In performing the assessments, The WRRO evaluates the implementation of proper cyber controls. These findings are shared with federal/state partners in a manner that protects security sensitive information from public disclosure. The WRRO minimizes the burden on federal and state partners while developing the information necessary to ascertain the cybersecurity posture of the sector.

   b. Would a traditional regulatory model -- run entirely by government regulators, including compliance inspections -- be cost effective or efficient? Why?

- We recognize that there is need to provide some level of standardization, accountability, and regulatory certainty as it pertains to cybersecurity in the water sector.
- We also recognize that EPA has very limited in-house capacity and expertise to support a robust cybersecurity program. Building that capability would not be in the best interest of the water sector, when an alternative and more nimble approach can be implemented leveraging non-federal resources to achieve the same mission. Likewise, states have limited capacity or technical expertise to sustain a regulatory oversight function.
- AWWA recommends that the WRRO be an independent, non-federal entity, that is self-sustaining through dues/fees and therefore will not require additional federal funding after it is established. An independent WRRO can effectively perform the task of developing requirements, assessing compliance and providing state/federal partners with those findings while protecting security sensitive information from public disclosure. More specifically, the vetting of the cyber requirements will undergo an in-depth stakeholder engagement process with subject matter experts in a manner that provides more flexibility and generates broader sectoral concurrence even before they are approved for compliance purposes.
- The traditional regulatory development process is typically more binary with one proposal developed by an agency for which the stakeholder community gets one opportunity to provide comment. The stakeholder community has no role in comment adjudication, which has often led to legal challenges of final rules.

5. You have stated that a digital transformation will require focused funding and clarification on what is or is not allowable under State Revolving Funds.
   a. Are there other ways to address legacy systems?
      - If the goal is expediting the transition from legacy systems that are inherently vulnerable, then some sort of targeted funding will be necessary.

   b. Without this funding, can there be overall sector advancement on cybersecurity?
      - The timeline for full transformation of operational technology can span 1-4 years, depending on the size and complexity of systems. Keep in mind that the utility must maintain full-service functionality during the overhaul period. In essence this is like changing the tires on a NASCAR while it circles the racetrack.
      - Without access to targeted funding, systems will have to continue to try to "do more with less" which will result in a slower transition and could leave systems vulnerable. Funding is necessary to overcome the growing digital divide and enable the most stressed systems to transition from legacy systems are or more vulnerable, receive the necessary training and skills development to maintain a workforce to support the system.

The Honorable Russ Fulcher

1. What do you recommend water systems use today as a flexible and up to date benchmark to address the government's interest in protecting our critical infrastructure? How are groups like yours and others supporting the water sector in this area?

- AWWA has developed essential planning resources to support water utilities on their path to cyber resilience. These are based on the NIST Cybersecurity Framework and have been designed to help a utility clarify their exposure to cyber risks, set priorities, and execute an appropriate and proactive cybersecurity strategy. All of these have been made available for free by AWWA.

  1. **Water Sector Cybersecurity Risk Management Guidance**. Practical, step-by-step guidance from AWWA for protecting process control systems used by the water sector from cyberattacks. Following this guidance saves time and yields more comprehensive, accurate and actionable set of prioritized recommendations from the Assessment Tool.
  2. **Assessment Tool**. This interactive tool asks utilities to examine how they are using various technologies. Based on responses, the tool generates a customized, prioritized list of controls that are most applicable to the utility's technology applications. Utilities can use this output to determine the implementation status of critical controls designed to mitigate cybersecurity vulnerabilities. Output from this tool can be uploaded into CISA's Cyber Security Evaluation Tool (CSET) to avoid duplication of effort.
  3. **Small Systems Guidance**. A getting-started guide to help small rural utilities improve their cybersecurity practices focused primarily on the needs of water utilities serving fewer than 10,000 people, and especially those serving fewer than 3,300 people. This resource was developed in collaboration with the USDA.

- CISA has developed a suite of resources that provide solutions to myriad cybersecurity challenges. The CISA Vulnerability Scanning Service is likely of highest immediate value to all systems, especially those with limited in-house capacity. We should have a nationwide messaging campaign spanning several months to maximize enrollment. This may be one of single most valuable resources in which a utility could enroll to receive immediate benefit in assessing external vulnerabilities to their system.

The Honorable Nanette Barragan

1. Since the Bioterrorism Preparedness Act of 2001, water systems serving more than 3,300 persons have been required to conduct a vulnerability assessment and prepare an emergency response plan, which was directed to include cybersecurity threats. Then, in 2014 under Executive Order 13636: Improving Critical Infrastructure Cybersecurity, the National Institute of Standards and Technology created a framework, and AWWA issued guidance that provided actionable steps to improve cybersecurity. Now ten years later we are still seeing water systems facing increased cyber threats. The EPA has now withdrawn their March 2023 cybersecurity rule mandating that cybersecurity audits be part of the sanitary surveys. How would you suggest the government provide water systems with the support, both financially and systematically needed to address the cybersecurity challenges immediately facing water systems?

   - The government can provide water systems with support by authorizing the establishment/identification of a Water Risk and Resilience Organization (WRRO), a sector-led entity, to develop, implement and enforce cybersecurity risk and resilience requirements for drinking and wastewater systems. As designed, the WRRO will work in close partnership with EPA, while bringing sector-specific experience and know-how to effectively and efficiently protect the nation's water infrastructure from cybersecurity threats. The proposed legislation authorizing the WRRO is inspired by the successful model implemented in the U.S. electric sector. The proposal leverages on-the-ground expertise in the water sector, reimagines the current administrative top-down approach to cybersecurity which has proven inefficient and ineffective, and sets the water sector on a path towards robust cyber maturity.

- Targeted funding is necessary to support expedited implementation of cybersecurity controls and a transition from legacy technology. The Drinking Water and Clean Water State Revolving Funds, the Water Infrastructure Finance and Innovation Act (WIFIA) program, and other authorized EPA programs, along with USDA Rural Development grants, can provide important and timely funding for cybersecurity projects. Defining eligible cybersecurity activities is necessary, which includes addressing constraints that may inhibit funding of various cybersecurity controls.

2. Regarding federal funding, your testimony references constraints on the State Revolving Loan Fund program that limit how useful this fund is for cybersecurity upgrades. What constraints are you referring to, and are there actions Congress or the administration can take to make these funds more flexible?

- .The water sector lacks a dedicated funding program to support the replacement of legacy systems with inherent cybersecurity vulnerabilities. Current programs managed by EPA and USDA can be used for cybersecurity projects but must compete with a wide array of needs. A dedicated funding program would help to address the digital divide at a time when our adversaries are expanding their capabilities is necessary to prioritize replacement of legacy systems. This includes appropriating the funding authorized in America's Water Infrastructure Act of 2018 that was intended to support the risk and resilience management efforts of drinking water systems.

- The State and Local Cybersecurity Grant Program (SLCGP) managed by CISA is in the early stages of deployment. While the cybersecurity needs of drinking water and wastewater appear to be eligible, it remains to be seen if any funding will be awarded to the water sector by states administering the program. While CISA has stated that cybersecurity in the water sector is a high priority, the guidance provided for SLCGP implementation offers no such prioritization criteria to inform funding allocations by the state programs. Therefore, the effectiveness of this program in addressing some of the cybersecurity needs of water utilities is currently unknown.

- A key challenge for the most disadvantaged systems is their capacity to actually develop and submit a funding request to any of the available programs. Technical assistance to support applications is a key factor in overcoming the digital divide will continue to grow as utilities with legacy systems face competing priorities to satisfy new regulatory obligations on drinking water and wastewater operations that strain budgets that are 100% dependent on ratepayers.

- Finally, providing clearly defined eligibility criteria for cybersecurity activities is necessary to provide certainty on the applicability of existing funding programs or those developed in the future to support implementation of various cybersecurity controls. Currently there is a degree of uncertainty that may inhibit the effective application of funding programs to support cybersecurity objectives. EPA, USDA and CISA should establish a workgroup with water utilities to review a series of prospective cybersecurity projects that a utility might implement to address legacy systems, identify constraints with funding program eligibility and what authorities may need to be changed to support more effective application of the funds relative to water utility needs and overall cybersecurity risk management objectives.

3. What federal initiatives are currently in place to enhance intelligence-sharing within the water sector, and is there more than can be done?
    - Improved functionality and collaboration between federal partners and water sector subject matter experts via the WaterISAC is essential to assess the applicability and relevance of cyber threat information to water sector stakeholders, including clarity on actions to be taken. EPA should partner with the sector to expand awareness of and access to these resources.