House Subcommittee on Environment, Manufacturing, and Critical Materials
Hearing Entitled, "'Ensuring the Cybersecurity of America's Drinking Water Systems."
January 31, 2024
Questions for the Record for Scott Dewhirst

The Honorable Earl L. "Buddy" Carter

1. Your testimony put forward the approach for cybersecurity taken by the electric sector as one model that could be replicated in the water sector to ensure public water systems carry out appropriate cybersecurity best practices.

    a. Can you expand on how that model could work in the water sector?

    Response: Applied to the water sector, this model would have a co-regulatory body like the North American Electric Reliability Corporation (NERC) for the electric sector. This body could be an appointed group of water and cybersecurity sector experts or a third-party entity identified through a qualifications based selection process. This body would develop a suite of tiered, risk-based cybersecurity standards and best practices appropriate for water systems of various sizes and risk profiles. Through federal oversight, water systems would be required to abide by the standards demonstrated through an audit process, and could be offered funding and technical assistance to achieve these benchmarks. However, the program would not allow EPA or any other federal agency to require water systems to take any specific cybersecurity action but rather identify gap(s) and allow the co-regulatory body to adopt standards to address those gap(s).

    b. Do you believe it should be an exact replication of the electric sector's approach, or are there aspects of that approach that would not transfer well to the water sector?

    Response: No, there are several requirements of the electric sector approach that seem overly burdensome and are of limited value for the water sector. The first is recordkeeping. It is my understanding the electric sector requires recordkeeping to demonstrate compliance each and every day between audits. Rather, the water sector can take an approach like the payment card industry (PCI) and require compliance with a point-in-time audit. Utilities should adopt practices and standard procedures that will achieve the desired outcome of secure business and control systems and demonstrate their application during the audit process.

    Second, the North American Electric Reliability Corporation (NERC)-glossary of terms is overwhelming in size and any such reference for the water sector should be simplified. As shared during the testimony, there are approximately 50,000 community drinking water systems across the county,

about half of which serve fewer than 500 people, compared to approximately 3,000 electric utilities. Couple this with the more isolated nature of water utilities compared to the much greater degree of interconnectedness required to operate the bulk electric system and a less rigorous approach is needed.

Finally, it is important to not use prescriptive language but rather focus on desired outcomes. An example is saying prescriptively utilities shall patch their systems daily; rather state systems shall be monitored and patched on a consistent basis in alignment with risk exposure.

2. If you had complete autonomy to set up the Federal government's efforts concerning addressing cybersecurity in the water and wastewater sector, how would you arrange things on the Federal side to best help the sector?

Response: The testimony offered at the hearing was generally aligned and valuable input was received from everyone represented. To start, I would stand-up a task force with representatives from the entities at the hearing to put together an approach modeled after the electric sector that could be supported by the water sector and EPA with a defined outcome to ensure cyber and physical security of the nation's water infrastructure. This could be accomplished in several facilitated workshops involving representatives with the authority to speak on behalf of those entities. I would then invite individuals responsible for NERC-compliance from the electric sector to provide feedback on the approach developed. Once that feedback is addressed, I would solicit comment from the water sector at large to finalize the approach that could then be reviewed and shared with EPA for implementation.

The Honorable Rick W. Allen

1. Could you share the importance of having the standards for the water sector developed primarily by the sector itself, including sector experts?

Response: It is critical that the standards developed for cybersecurity of the sector understand the control systems and practices used to operate water utilities. If standards are adopted that are impractical or overly burdensome to meet, they may be circumvented or simply not adopted resulting in unaddressed vulnerabilities. Sector knowledge is also essential given the wide range in size and complexity of water systems across the nation. Rather than having the federal government mandate certain actions in a regulatory capacity, best practices and standards developed by the sector could be more precisely tailored to reflect the needs and capabilities of water systems with different risk profiles. The focus should be on outcomes and not a prescriptive, one-size fits all approach. Sector-developed standards would also have a higher degree of buy-in from members of the sector and would present an opportunity for entities like WaterISAC to work with

individual water systems to facilitate adoption of these practices. Further, rural systems are generally best supported by those whom they know and trust and are less receptive and trusting of outside, unknown third parties regardless of their expertise.

a. Should EPA be able to overrule the recommendations or guidance of the sector, including the people on the ground who have experience with these issues?

Response: No, it would not be wise to allow EPA to overrule the sector's recommendations on cybersecurity practices. Using the NERC model as an example the regulator, Federal Energy Regulatory Commission, issues a Notice of Proposed Rulemaking and NERC then develops a standard that addresses the concern and takes into consideration specific sector operational knowledge. The co-regulatory body for the water sector would act in a similar manner to a concern from EPA. Neither a utility nor EPA nor our state primacy agencies want a failure of any kind because of the trust that would be eroded so there is inherent accountability. The co-regulatory body also is staffed with cyber experts and those with an understanding of utility operations so should be well suited to address the concerns of EPA and thus making it unnecessary for EPA to mandate action or overrule a practice. EPA is generally best suited and structured to regulate drinking water quality standards.

The Honorable Russ Fulcher

1. During my questions, I noted the Idaho National Laboratory (INL) is not only testing how degraded piping and other degraded water infrastructure can undermine the ability of chlorine to prevent the regrowth of bacteria and pathogens. That morphed into a cybersecurity discussion due to INL's having a Water Security Test Bed (WSTB) to mimic a city water system at its site of research and test countering cyberattacks that try and "spoof" water quality readings, providing false readings to the operator and thus sending contaminated water to users in a community.

    a. How much do water systems think about protecting themselves from their control structure being tricked so that it continues to feed contaminated water to consumers?

    Response: While I do not want to speak too specifically to the potential threat you identified, I will say that in general water utilities use a matrix of water quality parameters to gauge delivery of quality drinking water to the public. I would expect that some sort of breach that you reference would show itself in another area of that matrix and operational staff would be alarmed to this issue. Also systems may have a layered approach to monitoring such that multiple instruments and/or devices would need to have a coordinated breach to truly spoof operators. With appropriate cybersecurity standards

such a breach would be unlikely and that should be the focus.

b. What types of steps does the sector need to take to address issues like this?

Response: As alluded to in the prior response, layered monitoring systems and utilizing a matrix of water quality parameters helps to alarm operators of potential issues. Most control systems have pre-set alarms to alert staff when things are not within normal, expected ranges so that appropriate corrective measures can be employed.

2. The EPA Office of Research and Development's Water Security Test Bed located at Idaho National Laboratory is a national asset for probing water system vulnerabilities. Is there value in having a facility for large- scale testing of cyber-physical vulnerabilities in water systems that can also evaluate interdependencies with other critical infrastructure (e.g., electrical grid)? Where do industry and utilities need help to secure America's drinking water systems? What are the gaps that government R&D can help address? To better understand how adversaries are threatening our water sector, is there value in providing an objective forum (e.g., at a National Laboratory) for public-private partnerships to address systemic risks, destructively test scenarios, and train utilities and operators?

Response: I believe that cyber threats are often not specific to a particular industry and attackers are simply looking for any vulnerable system(s) and happen upon those that are not protected adequately. Actionable guidance for water utilities is readily available (such as WaterISAC's *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*) and if implemented universally would go a long way toward protecting utility systems. I believe establishing standards and implementing them in a risk-based approach is the first step to protecting our sector; the measures you reference could be considered as the cybersecurity maturity of the sector grows and the attacks become more sophisticated.

The Honorable Frank Pallone, Jr.

1. At the hearing, we heard concerns that aging operational technology may not work with newer enterprise platforms, forcing some systems to consider overhauling their operational technology.

a. How can EPA and other appropriate federal agencies help bridge the gap?

Response: Additional funding assistance from EPA would be welcomed by the water sector to offset the costs of updating operational technology. For example, if a new cyber oversight model for the sector resulted in a recommendation or a requirement for certain water systems to adopt operational technology that meets minimum cyber performance requirements, then EPA could offer grant or low-cost financing assistance to

facilitate adoption.

b. Are additional federal resources or guidance needed to address this issue?

Response: Yes, and it could start with increasing annual appropriations for authorized EPA programs intended to help community water systems improve their cyber posture. For example, in 2021 Congress authorized the Midsize and Large Drinking Water System Resilience and Sustainability Program, which will offer grant assistance to help community water systems defend against risks including cyber-attacks. While it was authorized to receive up to $50 million per year, to date only a little more than $7 million has been appropriated to the program. Additionally, in 2018 Congress authorized the Drinking Water Infrastructure Risk and Resilience Program through which EPA would offer grants to help community water systems increase resilience to a variety of vulnerabilities, including those to electronic and computer systems. But the program was never funded and expired after the 2021 fiscal year.

The Honorable Nanette Barragan

- Your testimony referenced the advantages Tacoma Water has as a division of Tacoma Public Utilities alongside Tacoma Power, to leverage cybersecurity tools for both your electric and water systems. Are there best practices that Tacoma Public Utilities has used to improve cybersecurity for all its systems which other water utilities that offer more than one service can learn from?

Response: All utilities, regardless of their organizational structure, can take advantage of the *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* guidance developed by WaterISAC. In the case of Tacoma Water, we take advantage of economies of scale in that we leverage the investment made in enterprise grade cyber tools shared with Tacoma Power. These tools monitor communications from across the network to identify potential vulnerabilities. This includes end point detection and response; logging who or what device the system has communicated with and alarm if outside of the immediate geographic area. Some of our practices also include vulnerability management meaning that we typically scan daily for unusual activity and patch vulnerability weekly, or as risk dictates. We also utilize tools that establish a protocol break so when you are accessing the control system, you are not actually "in" the system but rather operating in an overlay layer so as to not expose the actual control system to outside access. Another key component of our system is the architecture of the network, utilizing segmentation and isolation such that no control system is "on the internet."