

Testimony of Cathy Tucker-Vogel

Past President of the Association of State Drinking Water Administrators

Public Water Supply Section Chief, Kansas Department of Health and Environment

to the

Subcommittee on Environment, Manufacturing, and Critical Materials

House Committee on Energy and Commerce

Ensuring The Cybersecurity Of America's Drinking Water Systems

Wednesday, January 31, 2024



Executive Summary

Water utility cybersecurity is critical for providing safe drinking water and protecting public health. Solutions to improve the cybersecurity posture of the sector must incorporate both assessments & corrective actions, supported by adequate funding for both.

States will have to play a role in any future cybersecurity approaches. Several states are currently using a variety of approaches, both regulatory and non-regulatory, to improve cybersecurity, and any Federal actions should incorporate the lessons learned from these approaches, not supersede them, and harmonize with ongoing approaches.

Any future Federal actions on cybersecurity in the water sector must take feasibility into account. EPA's recently withdrawn memorandum highlighted significant gaps within the water sector's ability to address cybersecurity. These feasibility concerns must be considered and should be addressed before meaningful progress can be made. These issues include:

- A lack of sufficient funding for both states and systems
- A wide range of subject matter expertise at state drinking water programs or at Public Water Systems (PWSs)
- The frequency of assessments must align with the ever-evolving nature of cyber threats
- Many states lack sufficient authorities to protect sensitive critical infrastructure information that would present a cyber risk if made public.

Any future Federal actions on cybersecurity must be developed in collaboration with the co-regulators, i.e., state agencies and the regulated entities, i.e., the water systems. Cybersecurity is not a contaminant that can be addressed through the traditional SDWA regulatory development process with a Maximum Contaminant Level (MCL) or Treatment Technique (TT). Given the diversity and the number of Community Water Systems (CWSs), an innovative approach is needed that goes beyond EPA's traditional approach for regulations. The SDWA's regulatory framework was not designed for an approach for cybersecurity, so creative, collaborative solutions are required.

Testimony

Good Morning Chair Rodgers and Ranking Member Pallone, Subcommittee Chair Carter and Ranking Member Tonko. Thank you for this opportunity to come before you and discuss how the Federal government can appropriately with the state drinking waters and the balance of the water sector to ensure the cybersecurity of the country's water systems. Cybersecurity across the water sector has many complex technical and institutional challenges, and a focused, collaborative effort is needed to meet these challenges.

My name is Cathy Tucker-Vogel, and I am a Past President of the Association of State Drinking Water Administrators (ASDWA), whose 57 members include the 50 state drinking water programs, five territorial programs, the Navajo Nation, and the District of Columbia. ASDWA's members and their staff are the scientists and the engineers on the front lines every day, implementing the SDWA by providing compliance oversight, technical assistance and enforcement, or primacy, for drinking water systems. I testified previously before the Subcommittee in February 2020 on lead and copper. I also served on the State-EPA Water

Sector Cybersecurity Workgroup that provided advice in 2022 on EPA's March 2023 cybersecurity memorandum

I am the Public Water Supply Section Chief at the Kansas Department of Health and Environment (KDHE), where I have worked for over 30 years. I oversee statewide programs that implement the Safe Drinking Water Act (SDWA) through regulation of public water supply systems, including compliance and enforcement determinations, providing technical assistance, implementation of the Drinking Water State Revolving Loan Fund (DWSRF), operator certification, and many other programs to ensure safe drinking water.

Today, I will discuss ASDWA's perspective on cybersecurity in the water sector. Cybersecurity has been a challenging issue for water systems for a variety of reasons, starting with the diversity and the number of Community Water Systems (CWSs). The water sector is unlike other utility sectors of critical infrastructure that have a smaller total number of entities, as well as many of the other sectors being primarily private, for-profit companies. The water sector has approximately 50,000 Community Water Systems (CWSs), with the vast majority being governmental entities, i.e., not-for-profit, and broken down by system size as shown below:

- 1,048 large systems serving greater than 50,000 people
- 8,402 medium systems serving 3,301-50,000 people
- 39,889 small systems serving 25-3,300 people

Note that there is an unknown percentage of small systems that operate based on pressure in the distribution system, so are stand-alone and not connected to the internet. In addition, approximately 40,000 non-community, non-transient water systems, such as separate schools, factories, etc., are not connected to CWSs and have their own small system – the percentage of this class of systems that are not connected is also unknown. Our collective understanding of the breadth and depth of the cybersecurity vulnerabilities across the water sector is unknown due to the lack of inventory data for systems connected to the internet. This lack of inventory data impacts the ability of the sector to effectively target solutions and improvements tailored to different system sizes and resources.

All water systems face challenges with aging infrastructure and aging workforce, as well as the increasing costs of compliance with regulations, especially upcoming regulations such as the regulation for Per- and Polyfluoroalkyl Substances (PFAS) and the Lead and Copper Rule Revisions/Improvements. Small systems are especially challenged by the lack of resources to balance and prioritize the competing priorities, including cybersecurity.

The start of cybersecurity in the water sector goes back to the Vulnerability Assessments (VAs) required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188), also known as the Bioterrorism Act. This legislation required water systems serving greater than 3,300 people to review “the current and future methods to prevent, detect and respond to the intentional introduction of chemical, biological or radiological contaminants into community water systems and source water for community water systems, as specified”. The legislation also required “the review of methods and means by which terrorists or other individuals or groups could disrupt the supply of safe drinking water or take other actions against water collection, pretreatment, treatment, storage and distribution facilities which could render such water significantly less safe for human consumption, as specified”. These requirements were the first experience for a large number of systems to conduct VAs and develop robust Emergency Response Plans (ERPs) based on what was learned from the potential threats and consequences from potential loss of critical system assets.

The Bioterrorism Act was developed in response to the 9/11 terrorist attacks, and logically focused on physical threats and contamination. Cybersecurity was discussed as part of the various vulnerability assessment processes, but cybersecurity knowledge and the breadth of cybersecurity threats have evolved significantly over the last two decades.

As a result of the Bioterrorism Act, state agencies received additional funding for a few years for security coordinators that resulted in an improved security profile across the water sector. It should be noted that no additional funding was made available to the water systems to make any of the security improvements identified by the vulnerability assessments. Water systems prioritized potential improvements and focused on physical security such as fencing, access control, etc., and some limited cybersecurity improvements based on limited knowledge, as well as improving emergency preparedness and response.

An important outcome of the evolution in water security and preparedness was the formation of [Water and Wastewater Response Networks \(WARNs\)](#) across the country, essentially modeled after the response network for electrical utilities. The WARNs focus on utilities helping utilities and have been extremely effective in response to extreme weather events such as hurricanes, floods, tornadoes, wildfires, etc., by moving people, equipment, and supplies to the impacted area in a short period of time. The WARNs are exploring appropriate responses to cybersecurity attacks.

Cybersecurity was again addressed in America's Water Infrastructure Act of 2018 (AWIA, P.L. 115-270). AWIA required community water systems serving more than 3,300 people to develop or update their assessments and response plans. The law specified using an all-hazards approach for both natural and man-made threats that the risk and resiliency assessments (RRAs) and ERPs must address, including cybersecurity. The law established deadlines for water systems to certify to EPA the completion of the RRAs and ERPs and required periodic updates of the VAs and ERPs. Like the original regulatory requirement in the Bioterrorism Act for VAs and ERPs, AWIA is just an assessment and there is no audit function. However, the regulatory requirement was a thought-provoking tool that naturally should have been used to start the process of a true assessment of a system's cybersecurity vulnerabilities, i.e., "Hey, we have identified a problem. Where are the resources to resolve it?"

Water utility cybersecurity is critical for providing safe drinking water and protecting public health and must be done appropriately in a two-step process (assessments (RRA) & corrective actions), supported by adequate funding for both. Utilizing both vulnerability assessments and risk and resiliency assessments are the initial steps to improving cybersecurity and this approach has broad agreement across the sector.

Any national approaches to cybersecurity must harmonize with existing state approaches, to avoid duplication of effort or confusion, and allow sufficient flexibility to enable primacy agencies to engage effectively with PWSs.

Without coordination with state primacy agencies, a comprehensive, sector-wide response to promoting cybersecurity at PWSs is impossible. As co-regulators, state primacy agencies have regulatory oversight authority to ensure systems' compliance with the National Primary Drinking Water Regulations (NPDWRs). Further, primacy agencies have experience supporting system capacity beyond the focus on regulatory compliance. To that end, despite the lack of a collaborative and coordinated national effort, some state primacy agencies have developed or

expanded regulatory and non-regulatory approaches to improving cybersecurity at PWSs based on available resources and authorities.

Given the variability in program capacity and authority, most primacy agencies promote non-enforcement-based voluntary approaches - encouraging self/third-party assessments, connecting PWSs with available resources, and offering annual training opportunities. Generally, state primacy agencies are concerned with enforcing a strict regulatory framework due to variability in subject matter expertise in their program, insufficient protection of sensitive critical infrastructure information, and technical and financial resources to support the implementation of corrective actions. Still, several states are leading with more robust and innovative approaches.

For example, in New Hampshire, the drinking water program has leveraged funding from the American Rescue Plan Act (ARPA, P.L. 117-2) to set up a grant that offers financial assistance to systems that conduct cybersecurity assessments. The funds can then be used for corrective actions that may be identified during the assessment. Other states may provide educational materials or incorporate simple questions to gauge the cyber resiliency of systems they engage during inspections as one method to identify those systems who may require additional support or assistance, and then work to connect them with existing technical assistance. While these are voluntary approaches, the focus is on identifying vulnerabilities with an emphasis on supporting corrective actions, ensuring that these approaches effectively improve the cybersecurity posture of these systems.

Since September 2021 when EPA announced their intention to include cyber assessments in sanitary surveys, Kansas has worked to develop an alternate program that helps ensure public water supply (PWS) systems are taking the actions necessary to defend against cyber-attacks. The Kansas Drinking Water Program in partnership with the Kansas Information Security Office (KISO) and the Cybersecurity and Infrastructure Security Agency (CISA) have developed an electronic assessment tool that will be used by Kansas public water supply systems to identify cyber vulnerabilities. We worked closely with our partners to create our assessment tool using the Cybersecurity Performance Goals (CPG) developed by CISA.

Our assessment program includes four phases. Phase One, started in January 2024, includes outreach and training to water operators explaining our assessment program and the importance of robust cybersecurity hygiene to defend against cyber-attacks that could disrupt water treatment operations. Phase 2 will require PWS operators to complete a short 3-4 question electronic survey which will identify water systems that have operational technology. Phase 3 will require all PWS systems that have operational technology to complete an electronic assessment based on CISA's CPG Checklist. Phase 4 includes follow-up and technical assistance from CISA and or KISO for PWS systems with cybersecurity vulnerabilities identified during the evaluation completed in Phase 3.

KDHE will require PWSs to complete cybersecurity assessments annually. This will provide data to track water system improvements in cybersecurity implementation over time. The electronic reporting application used by KDHE is not publicly available and the data collected is not subject to the Kansas Open Records Act. This protects sensitive information that could jeopardize water system operations if made public.

Considerations for Future Approaches

EPA's recently withdrawn memorandum exceeded the water sector's capacity and raised significant implementation concerns. States' concerns with this approach were repeatedly raised in three letters (8/25/21 to Jennifer McLain, 9/22/21 to Radhika Fox, 2/9/22 to Radhika Fox) that have been included as appendices to this testimony. The sector, collectively, must reflect on the considerations from those letters, which are detailed below, when evaluating any future approaches.

Funding is necessary for both states and systems to appropriately address cybersecurity

As previously mentioned, as a result of the Bioterrorism Act, state agencies received additional funding for a few years for security coordinators that resulted in an improved security profile across the water sector while that funding was in place. States would need a consistent source of new cybersecurity funding to restart raising the profile of the water sector. This funding must be new and cannot be taken from current funding sources, such as the Public Water Supply Supervision (PWSS) or the Drinking Water State Revolving Loan Fund (DWSRF) set-asides. The importance of cybersecurity warrants new funding.

Similarly, water systems have struggled to find the financial resources for cybersecurity. While some cybersecurity fixes such as two-factor authentication do not require significant resources, other cybersecurity fixes are expensive. For example, if an operating system needs to be upgraded, then, in some cases, new Programmable Logic Controllers (PLCs) are necessary throughout the treatment and distribution system to be compatible with the new operating system. Some of the technical complications for cybersecurity improvements require significant investments. Systems will also need a new source of funding for cybersecurity improvements.

The subject matter expertise at state drinking water programs or at Public Water Systems (PWSs) varies significantly between the programs and the systems

While some state primacy agencies were able to hire a cybersecurity coordinator, engage with a contractor, or leverage other state-wide resources, e.g., their local Cybersecurity and Infrastructure Security Agency (CISA) representatives, most state primacy agencies lack the necessary technical skills and knowledge to assess the adequacy of a system's cybersecurity measures effectively. Ensuring water systems are progressing in implementing controls identified in corrective action plans requires subject matter experts to provide ongoing support to those systems that need the most assistance moving through their path. While training is available, the current training is insufficient to turn these individuals into the necessary subject matter experts that this threat requires. Qualified cybersecurity experts use years of training and experience to provide the appropriate advice and services.

Cybersecurity is a field that is constantly evolving, so that any training received is reflective of a moment in time. If the expectation is that existing state staff become subject matter experts, meeting this expectation would require constant training and engagement on the topic, occupying critical time that for many states would be added on top of existing duties. A similar problem exists for system operators, especially small system operators. Most water systems are run by staff without any science degrees, some of them are just high school graduates. States and water systems will have to hire cyber experts who are in high demand and command high salaries. Without dedicated funding, cybersecurity will fall on state staff who are overwhelmed with the implementation of existing and upcoming regulations.

The frequency of assessments must align with the ever-evolving nature of cyber threats.

Cybersecurity threats are constantly evolving and require fluid and versatile solutions. The frequency of cybersecurity assessments must be balanced. If assessments are required too frequently, there may not be sufficient time to evaluate new threats and refine the process. If the assessment frequency is too long, vulnerabilities may not be identified in a timely manner.

Many states lack sufficient authorities to protect sensitive critical infrastructure information that would present a cyber risk if made public.

Many state primacy agencies pursued non-enforcement approaches due to concerns over the protection of sensitive critical infrastructure information, as violations and enforcement actions are public information that may include vulnerabilities identified through assessments.

Information that details the cyber vulnerabilities of systems would provide a roadmap for potential cyberattacks by identifying at-risk systems. While a malevolent actor might not know the specific nature of the vulnerability, it would undoubtedly highlight the system as a potential target. Over time, the publicly available data would reveal the most vulnerable systems.

Potential liability concerns could be significant and are confusing.

The report of a cyber intrusion at Oldsmar, Florida, received widespread media attention and highlighted the need to increase the cybersecurity profile across the water sector. The investigation of this intrusion revealed that the water system had recently completed a federally mandated security risk assessment only months prior. This discovery not only calls into question the efficacy of these assessments but further raises concerns over the states' potential role in assessing or otherwise certifying a water system's cybersecurity posture. Knowing that primacy agencies lack cybersecurity fluency, if an intrusion event occurs after a cybersecurity assessment reveals no vulnerabilities, who is liable? Any actions taken on the federal level should partner with the water and wastewater sector to review existing cybersecurity tools that require updating and develop effective methods of assessing potential cyber risk and sound mitigation strategies.

Moving From Assessments into Corrective Actions

Even the most comprehensive assessments do not address deficiencies. A framework that supports corrective actions must be in place to assist these systems in addressing the identified problems during these assessments.

Any future Federal actions on cybersecurity must be developed in collaboration with the co-regulators, i.e., state agencies and the regulated entities, i.e., the water systems. ASDWA is moving forward with the planning for a potential collaborative approach that could result in a definite path forward to improve cybersecurity. Cybersecurity is not a contaminant that can be addressed through the traditional SDWA regulatory development process with a Maximum Contaminant Level (MCL) or Treatment Technique (TT). Given the diversity and the number of CWSs, an innovative approach is needed that goes beyond EPA's traditional approach. The SDWA's regulatory framework was not designed for an approach for cybersecurity, so creative, collaborative solutions are required.

A range of potential regulatory and non-regulatory actions should be considered through such a creative, collaborative process. ASDWA is amid the planning such a process. For example, operator certification programs that already include continuing education requirements could be updated with cybersecurity training to raise the cybersecurity profile. Capacity development programs could be

modified to include cybersecurity. Asset management programs could be modified to include cybersecurity, since Operational Technology (OT) and Information Technology (IT) assets warrant continual upgrades and maintenance like pumps, pipes, and valves. States that have training requirements for governing boards could be updated to include cybersecurity.

Appropriately training system operators on cybersecurity should be added to operator certification programs. Cybersecurity awareness should be added to technical, managerial, and financial (TMF) capacity for water systems. In addition to these two programs, EPA should partner with the state agencies that manage the State Revolving Funds (SRF)s to raise awareness about this issue. Last year, the Clean Water and Drinking Water SRFs provided financing to 2,683 systems in 2022, with 70% of those systems serving less than 10,000 people. This financing is an important touchpoint that is too often ignored or underutilized.

Another potential solution is a coordinated outreach campaign by all organizations on the Water Sector Coordinating Council (WSCC) and the Government Coordinating Council (GCC) to raise the cybersecurity profile, by emphasizing the starting point of appropriate network monitoring so that the sector can better understand which systems are vulnerable and which are not. Every potential communication channel should be used to advertise the existing cybersecurity tools and resources. The appropriate tools and resources exist, and more outreach is needed to increase the use of the tools and resources across the water sector

One example of a recently released tool is the [Cyber Hygiene Vulnerability Screening](#) by the Cybersecurity Infrastructure & Security Agency (CISA) that is provided free for any system that registers. Other equivalent network monitoring would provide a similar outcome. This outreach campaign would be a step in the right direction and more steps would evolve out the collaboration approach that ASDWA is planning.

As we participate in this hearing, ASDWA's members are working 24/7/365 to provide safe drinking water and protect public health, as problems with water systems do not follow an 8-5, Monday through Friday schedule. Cybersecurity is a critical component of their collective efforts. We look forward to keeping Congress informed of our progress, we truly appreciate this opportunity to provide our collective input from our 57 state and territory membership, and again we sincerely thank you for this opportunity to address cybersecurity in the context of states' oversight role for safe drinking water and improving public health protection.

Again, thank you Chair Rodgers, Ranking Member Pallone, Subcommittee Chair Carter and Ranking Member Tonko, and the other Members of the Subcommittee for this opportunity to appear before the Subcommittee.

Appendices

ASDWA 8/25/21 Letter to Jennifer McLain

ASDWA 9/29/21 Letter to Radhika Fox

ASDWA 2/9/22 Letter to Radhika Fox



August 25, 2021

Dr. Jennifer McLain
Director, Office of Groundwater and Drinking Water
U.S. Environmental Protection Agency
1200 Pennsylvania Avenue NW
Washington, DC 20009

Re: Cybersecurity Dialogue with the States

Dear Dr. McLain,

The Association of State Drinking Water Administrators (ASDWA) would like to continue the dialogue on cybersecurity with EPA in a timely manner, as cybersecurity has become a significantly greater risk to the over 150,000 public water systems (PWSs) in the past few years. We recognize the importance of the issue, the need to move beyond the status quo, and the need for a comprehensive strategic approach inclusive of critical Federal agencies such as the Department of Homeland Security (DHS). Increasing this dialogue as soon as possible is critical, as EPA needs to work closely with states to develop a better understanding of how water programs' cybersecurity challenges are being handled, and to help identify which types of resources and support would be most helpful to water programs and ultimately public water systems in the both the short and long term.

From ASDWA's perspective, the first substantive step in this dialogue is developing a mutual understanding of the expectations from any new cybersecurity efforts by EPA and the states. The enclosed list of ten questions from [EPA's Water Sector Cybersecurity Brief for States](#) is a starting point that quickly lead to implementation challenges when working in partnership to improve cybersecurity. For any of these questions, if the answer is "yes", then how is that answer verified? *Verification* aims to establish whether a *system* meets a set of requirements and it's not clear what the requirements are. On the other hand, if the answer is "no", then what is the next step?

Beyond the expectations, other challenging issues such as lack of knowledge on cybersecurity across the water sector, information security, potential liability, and others need to be addressed to determine which types of resources and support will result in improved

comprehensive cybersecurity. We look forward to setting up a few dates and times in the near future to delve into these important issues. Please feel free to email me at cathy.tucker-vogel@ks.gov or call me at (785) 368-7130 if you want to discuss how to move forward in a timely manner on this important issue.

Sincerely yours,

A handwritten signature in black ink that reads "Cathy Tucker-Vogel". The signature is fluid and cursive, with the first name "Cathy" and last name "Tucker-Vogel" clearly distinguishable.

Cathy Tucker-Vogel, ASDWA President
Chief, Public Water Supply Section
Kansas Department of Health & Environment

cc: Casey Katims-EPA OCIR
Yu-Ting Guilarian-EPA OGWDW
David Travers-EPA WSD
Dan Schmelling-EPA WSD



From EPA's Water Sector Cybersecurity Brief for States

1. Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility?

Never allow any machine on the control network to "talk" directly to a machine on the business network or on the Internet.

2. Segregate networks and apply firewalls?

Classify IT assets, data, and personnel into specific groups, and restrict access to these groups.

3. Use secure remote access methods?

A secure method, like a virtual private network, should be used if remote access is required.

4. Establish roles to control access to different networks and log system users?

Role-based controls will grant or deny access to network resources based on job functions.

5. Require strong passwords and password management practices?

Use strong passwords and have different passwords for different accounts.

6. Stay aware of vulnerabilities and implement patches and updates when needed?

Monitor for and apply IT system patches and updates.

7. Enforce policies for the security of mobile devices?

Limit the use of mobile devices on your networks and ensure devices are password protected.

8. Have an employee cybersecurity training program?

All employees should receive regular cybersecurity training.

9. Involve utility executives in cybersecurity?

Organizational leaders are often unaware of cybersecurity threats and needs.

10. Monitor for network intrusions and have a plan in place to respond?

Be capable of detecting a compromise quickly and executing an incident response plan.



September 29, 2021

Ms. Radhika Fox
Assistant Administrator for Water
U.S. Environmental Protection Agency
1200 Pennsylvania Ave. NW
Washington, DC 20460

Re: Cybersecurity in the Water Sector

Dear Ms. Fox,

Thanks for taking the time last week to meet with the ASDWA Executive Committee to discuss cybersecurity and the shared responsibility between the Federal government and states to make progress on this critical issue facing the water sector. We want to continue the dialogue with EPA over the next few weeks on the next steps needed to achieve the desired outcome of improving cybersecurity.

While we appreciate the need to improve cybersecurity in a timely manner, adding cybersecurity to sanitary surveys will not achieve the desired outcome for several reasons:

- Sanitary survey inspectors do not have the technical skills and knowledge to assess the adequacy of cybersecurity or make recommendations to resolve cybersecurity deficiencies. The inspectors review monitoring data and look at physical facilities, and that is their skill set. A few cybersecurity trainings are not going to make the inspectors into cybersecurity subject matter experts.
- At many water systems, the business and operating systems are linked to city government. Sanitary survey inspectors' authority to correct deficiencies does not extend to city government information technology systems.
- Sanitary surveys are required to be conducted either every three years or five years, depending on the system type. The need to be timely doesn't match up with the five years to obtain a baseline assessment of cybersecurity preparedness at water systems. Additionally, cybersecurity threats are constantly evolving which doesn't match up with three- or five-year cycles.
- States have liability concerns if a cyberattack occurs shortly after an assessment. Who is responsible in such a situation?
- In many states, the results of sanitary surveys are public information, including the deficiencies. This public information would provide a roadmap for potential cyberattacks by identifying at-risk systems.

Additionally, some states will have to amend statutes or regulations to address cybersecurity or sensitive information from sanitary surveys. These amendments would take time.

ASDWA leadership believes that Section 2013 of the America's Water Infrastructure Act (AWIA) of 2018 provides appropriate avenues for EPA to improve cybersecurity in a timely manner. We appreciate the opportunity to provide viable alternatives to sanitary surveys in improving cybersecurity in the water sector. The ASDWA Executive Committee looks forward to discussing these alternatives with you.

Sincerely,

A handwritten signature in black ink that reads "Cathy Tucker-Vogel". The signature is fluid and cursive, with the first name "Cathy" and last name "Tucker-Vogel" clearly distinguishable.

Cathy Tucker-Vogel

ASDWA President

Bureau of Water, Kansas Department of Health and Environment



February 9, 2022

Ms. Radhika Fox
Assistant Administrator for Water
U.S. Environmental Protection Agency
1200 Pennsylvania Ave. NW
Washington, DC 20460

Re: Cybersecurity Dialogue with the States

Dear Assistant Administrator Fox:

Throughout the second half of 2021, ASDWA has communicated both formally and informally with the Agency regarding our concerns with EPA's intention to issue a rule that newly interprets the requirements for sanitary surveys by primacy agencies to include cybersecurity. Our previous letter of September 29th (enclosed) detailed our concerns with this approach, and we want to re-emphasize our concerns with the lack of state subject matter expertise, potential liability, and confidentiality of information. As we see EPA continue to move forward to issue this rule in April as stated in its [Unified Agenda \(RIN: 2040-AG20\)](#), ASDWA would like to re-emphasize our desire to partner with the Agency and water and wastewater sector leaders to ensure a more durable and comprehensive cybersecurity response framework. EPA's planned approach is not going to work, and, collectively, we will find ourselves a year from now with limited improvement in cybersecurity for the water sector.

The goal of this letter is to request regular communications with EPA leadership on this critical issue. The last time ASDWA's members discussed cybersecurity with EPA was at the State-EPA Roundtable in late October 2021. The water sector needs EPA's leadership to develop an implementable cybersecurity program that uses the [Industrial Control Systems Cybersecurity Initiative – Water and Wastewater Sector Action Plan](#) as its foundation and will continue to improve cybersecurity across the water sector, beyond the first 100 days of the Plan.

ASDWA recommends that a hybrid cybersecurity program be developed that combines the subject matter experts (SMEs) from Federal agencies such as CISA for the assessments, with an extremely limited role for the "boots-on-the-ground" inspectors from the primacy agencies for any follow-up actions. The Agency's planned approach using sanitary survey inspectors puts all the burden of determining cybersecurity adequacy with state staff that have been trained to provide oversight on monitoring data and inspect treatment and distribution system facilities and are not cybersecurity experts. Simple yes/no cybersecurity questions (sample enclosed) may not have simple answers. With a "yes," how is adequacy determined? With a "no," how are next steps determined? SMEs need to conduct the assessments and determine next steps,

and EPA's planned approach to provide guidance and training will not transform state staff into cybersecurity experts.

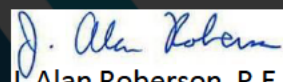
ASDWA has offered alternative programmatic options (enclosed) to EPA via a blend of EPA direct implementation under AWIA using subject matter experts (SMEs) and technical assistance providers, although this input has not led to a meaningful dialogue. Another hybrid option would be to provide funding for CISAs SMEs for assessments, and for inspectors to arrange the assessments and function as "go-betweens" for the SMEs. ASDWA recognizes that any hybrid option would take significant Federal resources, and other approaches warrant additional discussion.

ASDWA appreciates the Agency's acknowledgement of the immediate threat that inadequate cybersecurity poses to the sector, as well as its commitment towards lowering the sector's risk profile and protecting it from future threats through educational resources and the promotion of best practices. It is clear to primacy agencies that EPA understands the grave nature cyber-attacks pose to our collective mission of ensuring that all Americans have access to safe drinking water. Still, even as the frequency and sophistication of cyber-attacks on critical infrastructures continue to increase, the water sector needs a clear path forward that provides doable and durable cybersecurity.

To be clear, states are not objecting to our responsibilities as regulators to play a role in taking actions to enhance cybersecurity at public water systems. But SMEs need to have the lead role for assessments. States are under pressure to respond to the increasing threat of attack and, in the absence of Federal leadership or a clear understanding of the Agency's direction, some states are developing their own policies and guidance for systems. This state-by-state approach will only increase confusion and the complexity of future Federal actions to ensure consistency in implementation of any nationally derived cybersecurity response framework. If we are to address the immediate threat today while mitigating the impacts of the threats of tomorrow, a proactive and collaborative partnership is necessary – collaborate early and often.

ASDWA looks forward to working with EPA and the broader sector on strategies to address cybersecurity. ASDWA further encourages the adoption of a proactive approach through close coordination between the GCC and WSCC, who are best situated to lead the water sector in this effort, towards the development of a well-defined and nationally consistent cybersecurity response framework.

Sincerely Yours,



J. Alan Roberson, P.E.
Executive Director

Cc: Bruno Pigott and Navis Bermudez – EPA OW
Jennifer McLain and David Travers – EPA OGWDW
Ted Stanich – EPA OHS

September 29, 2021

Ms. Radhika Fox
Assistant Administrator for Water
U.S. Environmental Protection Agency
1200 Pennsylvania Ave. NW
Washington, DC 20460

Re: Cybersecurity in the Water Sector

Dear Ms. Fox,

Thanks for taking the time last week to meet with the ASDWA Executive Committee to discuss cybersecurity and the shared responsibility between the Federal government and states to make progress on this critical issue facing the water sector. We want to continue the dialogue with EPA over the next few weeks on the next steps needed to achieve the desired outcome of improving cybersecurity.

While we appreciate the need to improve cybersecurity in a timely manner, adding cybersecurity to sanitary surveys will not achieve the desired outcome for several reasons:

- Sanitary survey inspectors do not have the technical skills and knowledge to assess the adequacy of cybersecurity or make recommendations to resolve cybersecurity deficiencies. The inspectors review monitoring data and look at physical facilities, and that is their skill set. A few cybersecurity trainings are not going to make the inspectors into cybersecurity subject matter experts.
- At many water systems, the business and operating systems are linked to city government. Sanitary survey inspectors' authority to correct deficiencies does not extend to city government information technology systems.
- Sanitary surveys are required to be conducted either every three years or five years, depending on the system type. The need to be timely doesn't match up with the five years to obtain a baseline assessment of cybersecurity preparedness at water systems. Additionally, cybersecurity threats are constantly evolving which doesn't match up with three- or five-year cycles.
- States have liability concerns if a cyberattack occurs shortly after an assessment. Who is responsible in such a situation?
- In many states, the results of sanitary surveys are public information, including the deficiencies. This public information would provide a roadmap for potential cyberattacks by identifying at-risk systems.

Additionally, some states will have to amend statutes or regulations to address cybersecurity or sensitive information from sanitary surveys. These amendments would take time.

ASDWA leadership believes that Section 2013 of the America's Water Infrastructure Act (AWIA) of 2018 provides appropriate avenues for EPA to improve cybersecurity in a timely manner. We appreciate the opportunity to provide viable alternatives to sanitary surveys in improving cybersecurity in the water sector. The ASDWA Executive Committee looks forward to discussing these alternatives with you.

Sincerely,

A handwritten signature in black ink that reads "Cathy Tucker-Vogel". The signature is fluid and cursive, with the first name "Cathy" being more prominent and the last name "Tucker-Vogel" following in a similar style.

Cathy Tucker-Vogel

ASDWA President

Bureau of Water, Kansas Department of Health and Environment



Cybersecurity: Simple Questions with Simple Fixes

Cybersecurity is becoming a more significant risk in the water sector, and sanitary surveys are one potential option for improving cybersecurity. Sanitary surveys provide a flexible approach that builds off an existing program. Primacy agencies would have flexibility on what would be a significant deficiency versus a minor issue and how water systems would address deficiencies.

The inspectors would ask simple questions along these lines:

1. Is SCADA used? If yes, can the system operate if the SCADA system is disabled?
2. Is there a SOP for password management?
3. Does the system have remote access? If yes, is there a SOP for managing and protecting remote access? For example, are remote access credentials revoked when an employee leaves?
4. Is there an SOP for installing software patches and updates, and replacing outdated (unsupported) software?
5. Is there a SOP for basic cybersecurity training?
6. Is there a cybersecurity incident response plan?

If a system operator is unsure about the answer or the answer is insufficient or a more detailed cybersecurity assessment is needed, the system would be referred to a subject matter expert, either from EPA, DHS CISA, or a technical assistance provider.

Potential Drinking Water Cybersecurity Program

The America's Water Infrastructure Act (AWIA) gives EPA authority to do Cybersecurity assessments. AWIA Section 2013 requires community (drinking) water systems serving more than 3,300 people (10,251 systems) to develop or update risk assessments and emergency response plans (ERPs) that address the physical security and cybersecurity of the system.

Implementation of the AWIA requirements is through direct implementation by EPA.

Below is an outline for how a drinking water cybersecurity program might work under EPAs current authority:

- EPA develops CSAT (Cybersecurity Assessment Tool) similar to VSAT but focused on cybersecurity instead of all hazards. The CSAT should be based on the questions/guidance that EPA is developing for sanitary surveys – collect the same data, just with a different structure.
- PWS certify to EPA CSAT completed (same as AWIA now)
- Based on results of CSAT report the PWS will develop cyber SOPs, again based on EPA developed guidance
- PWS certify to EPA that cyber SOPs completed and implemented
- Under the National Compliance Initiative, EPA staff (or contractor) with cybersecurity expertise conduct on-site compliance inspections at selected PWSs each year.

This has the added benefit of getting the various Divisions (Security, OW, OECA) of EPA working together and interacting with states as a single agency instead of individually reaching out to states. Additionally, EPA would partner with CISA to develop training (both in-person and webinars) to water systems and technical assistance providers.

For the balance of community water systems that serve less than 3,300 people (approximately 40,000 systems), the states work to figure out how many small systems have SCADA and/or remote access by asking two questions:

1. Do you have a SCADA system?
2. Does anyone have remote access (operator laptop or any vendor access)?

If the answer is "yes" to either question, then pass on the system to a qualified third-party to conduct a cybersecurity assessment of the system – the third party could be a technical assistance provider such as RCAP or NRW (noting that NRW has signed an agreement with a cybersecurity provider - Mission Critical Global Alliance) or another organization. Similar to the large and medium systems, under the National Compliance Initiative, EPA staff (or contractor) with cybersecurity expertise conduct on-site compliance inspections at selected PWSs each year.

This could all be accomplished in a year or possibly, two years.