**TESTIMONY OF DAVID TRAVERS**
**DIRECTOR OF THE WATER INFRASTRUCTURE AND CYBER RESILIENCE DIVISION**
**U.S. ENVIRONMENTAL PROTECTION AGENCY**

**BEFORE THE**
**HOUSE ENERGY AND COMMERCE COMMITTEE**
**OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE**

**May 16, 2023**

Good morning, Chairman Griffith, Ranking Member Castor, and Members of the Subcommittee. I am David Travers and I serve as the Director of the Water Infrastructure and Cyber Resilience Division of the Office of Water at the U.S. Environmental Protection Agency (EPA). Thank you for the opportunity to speak to you today about the Agency's work with our partners to improve the security and resilience of America's water and wastewater systems to the persistent threat of cyber-attacks. This mission is among EPA's highest homeland security priorities.

As reported by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), critical infrastructure facilities, including water and wastewater systems, are being targeted for cyber-attacks with increasing frequency by both state-sponsored actors and criminal groups. Cyber-attacks on water and wastewater systems have stolen valuable financial data and customer information, destroyed essential information networks, and disabled communication systems. Recovery costs have ranged into the millions of dollars. More significantly, cyber-attacks can manipulate and disable the process control networks that are responsible for the treatment and distribution of water, which has the significant potential to endanger public health. Accordingly, the adoption of cybersecurity best-practices by water and wastewater systems to reduce the risk of these attacks is essential.

As you know, the federal government has identified 16 critical infrastructure sectors. Each of these sectors has a Sector Risk Management Agency (SRMA), which is the federal lead agency responsible for enhancing that sector's security and resilience against all hazards, including cyberattacks. By Presidential order, EPA serves as the SRMA for the water and wastewater systems sector due to our expertise in this area and the relationships we have cultivated with states and Tribes under the cooperative federalism of the Safe Drinking Water Act and Clean Water Act. Because the statutes allow EPA to treat Tribes as states, my discussion of "states" includes Tribes that are treated as states for purposes of these statutes. Multiple federal statutes, Directives, and Executive Orders mandate the Agency's cybersecurity mission.

The water and wastewater systems sector includes just under 150,000 public water systems (PWSs), which provide drinking water, and 16,000 publicly owned treatment works (POTWs), which treat wastewater, across the United States and territories. They range in size from serving less than 500 to more than 8 million customers. Small PWSs, meaning those that serve 10,000 people or fewer, make up 97% of all PWSs. Many small systems face challenges in reliably providing safe drinking water, including revenue shortfalls, aging infrastructure, and adequate staffing and expertise, and may lack the capabilities necessary to plan for and respond to natural and manmade threats.

EPA fulfills its critical mission in cybersecurity for the water and wastewater systems sector in coordination with DHS, the Water Sector Coordinating Council of industry representatives, and other federal, state, local, tribal, territorial, and private sector partners. EPA has worked with these partners for over 10 years to promote the adoption of cybersecurity best practices by water and wastewater systems through providing training, guidance, and technical assistance. I'm pleased to share with you several of these efforts.

- We have provided training on cybersecurity best practices, as well as threats, vulnerabilities, and incident response, to thousands of water and wastewater systems nationwide.
- Since 2017, EPA has provided direct individual technical assistance to water and wastewater systems using subject matter experts who help to assess the utility's current cybersecurity practices, identify gaps, and implement remediation actions to reduce risk that are tailored to the utility's resources and goals. To date, 235 utilities have participated in this program.
- To support water systems with cyber incident response planning, we have developed a *Cyber Incident Action Checklist* that guides utilities through preparing for, responding to, and recovering from a cyber-attack. This checklist has been incorporated into the Agency's *Water Utility Response On-the-Go* app to assist utilities when they cannot easily access the hardcopy versions of their emergency response plans.
- EPA understands the criticality of exercising emergency response planning and has created the *Water System Cybersecurity Tabletop Exercise* module to guide utilities with testing their readiness for a cyber incident. Additionally, we have conducted cybersecurity tabletop exercises for water systems at both the local and state level. The Agency has also developed the *Cyber Incident Response Plan Template*, which is currently under review by the Water Sector Coordinating Council, to assist water systems with building these sections within their existing Emergency Response Plans, recognizing that many small water systems will need a template to develop a strong plan.

- We continuously work in partnership with the National Security Council, including regular participation in the Cyber Response Group and other interagency work groups, to address cybersecurity policy issues and cyber incidents.
- EPA is currently partnering with the Water Sector Coordinating Council to craft the *Water Incident Severity Schema*, which will help the United States Government appropriately respond with the level of coordination and resources necessary to support water systems that are impacted by cyber incidents. A guide to cybersecurity insurance is under development as well.
- EPA consulted a workgroup comprised of the Water Sector Coordinating Council, Water Government Coordinating Council, and CISA to develop a *Prioritization Framework*, which describes a methodology for prioritizing public water systems for technical cybersecurity support and consulted with the workgroup again during the development of a *Technical Cybersecurity Support Plan* for public water systems, which is based on existing authorities of EPA and CISA for providing support to public water systems and the *Prioritization Framework*. EPA submitted the *Prioritization Framework* to Congress in May 2022 and the *Report to Congress Technical Cybersecurity Support Plan for Public Water Systems* in August 2022, pursuant to the Infrastructure Investment and Jobs Act SDWA amendment Section 1420A, *Cybersecurity Support for Public Water Systems*.
- Lastly, EPA has continued to request, identify, receive, and disseminate cybersecurity intelligence and cyber threat information relevant to the water sector through the EPA Federal Intelligence Coordination Office.

While EPA and its partners have achieved important gains in cybersecurity in the water and wastewater systems sector, the most significant cyber-risk in this sector is the continuing

failure of many utilities to adopt basic cybersecurity best practices. For example, in a self-reported 2021 survey of water systems conducted by water sector associations, only 31% of respondents had identified all their operational technology-networked assets, and just 22% had fully implemented cyber protections. Further, many reported incidents of cyber-attacks on water and wastewater systems have exploited this failure to implement cybersecurity best practices. Consequently, many water and wastewater systems remain highly susceptible to cyber-attacks that could disrupt their operations.

Due to this continued significant vulnerability of many water systems to cyber-attacks, the increasing frequency of cyber-attacks on critical infrastructure facilities, and the potentially significant public health impacts of a cyber-attack on a water system, EPA has leveraged its existing regulatory authority to improve cybersecurity in the sector. Accordingly, on March 3, 2023, EPA released a memorandum titled *Addressing PWS cybersecurity in sanitary surveys or an alternate process*. This memo was designed to ensure that all water systems are taking important steps to strengthen cybersecurity and to acknowledge that states have flexibility on how best to do this based on local needs.

The memorandum conveys EPA's interpretation of its existing regulations that states must include cybersecurity when they conduct regular audits of water systems through sanitary surveys or an alternate process. State sanitary surveys provide the fundamental touchpoint between the government and water systems through which states ensure that water systems are providing safe drinking water. Sanitary surveys are utilized to protect water utilities from physical vulnerabilities, and they should also be used to address modern cyber threats. Using this existing authority is essential to quickly strengthen this sector's cybersecurity across the nation.

At the same time, EPA acknowledged that state co-regulators have flexibility in how they implement the relevant regulations. By confirming and supporting state flexibility, EPA took a balanced approach to quickly and meaningfully reduce cybersecurity risks while avoiding inflexible, uniform, and costly requirements for states and water systems. EPA clarified that under its regulations, states may choose from three options when evaluating cybersecurity:

1. States may allow water systems to conduct a self-assessment or third-party facilitated assessment prior to the sanitary survey and then review the findings during the sanitary survey for unaddressed gaps that may represent significant deficiencies.
2. States may conduct the assessment while performing the sanitary survey in a traditional inspection format.
3. States may use an alternative program to conduct the assessment, but it must be as stringent as the sanitary survey program, occur no less frequently than the sanitary survey, and address gaps consistent with the significant deficiency process described in EPA's regulations.

The use of sanitary surveys to improve cybersecurity at water systems augments, and does not duplicate, the cybersecurity provisions in the 2018 America's Water Infrastructure Act (AWIA). First, EPA's interpretation of its regulations as described in the memo applies to all water systems, rather than the subset of community water systems subject to AWIA. Second, when a state evaluates the adequacy of the cybersecurity for producing and distributing safe water as part of a sanitary survey or alternate program, the state provides an assessment that is independent of the one performed by the water system under AWIA. Third, if the state identifies a significant deficiency in cybersecurity during a sanitary survey or alternate program, the water system must take necessary corrective action to address the deficiency, which is not the case for

risks or other vulnerabilities identified by a water system under AWIA. Water systems that developed risk and resilience assessments and emergency response plans under AWIA may, however, use these documents to support the evaluation of cybersecurity during their sanitary surveys or alternate program.

The approach of using sanitary surveys to assure cybersecurity at water systems has additional benefits. It retains the principle of state oversight of water systems; offers significant flexibility and support to states in how cybersecurity at water systems is evaluated; gives states the discretion to determine when a cybersecurity gap at an individual water system is a significant deficiency that must be addressed; and allows the state to work with the water system to develop a tailored site-specific solution to correct the cybersecurity gap. Moreover, relying on an existing regulatory structure allows for immediate implementation rather than the years-long process that developing a new regulation would entail.

EPA appreciates that while some states have established programs to evaluate water system cybersecurity practices, many states currently have less capacity to assist water systems in building protections against cyber threats. Consequently, EPA is providing guidance, training, and technical assistance, as briefly summarized below, to help states assess cybersecurity at water systems through sanitary surveys or an alternate program and to aid water systems with implementing cybersecurity best practices. These resources, as well as additional information supporting cybersecurity at water systems, are available at https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector.

- **Guidance.** EPA has published a primary guidance document, *Evaluating Cybersecurity in PWS Sanitary Surveys*, to help states and water systems assess cybersecurity for critical gaps, including potential significant deficiencies, and select remediation actions

appropriate for the capabilities and circumstances of the water system. EPA developed this guidance using the CISA *Cybersecurity Performance Goals*. Additional guidance covers the protection of security-sensitive information, potential funding, including EPA's *Drinking Water State Revolving Fund* and the CISA *State and Local Cybersecurity Grant Program*, and other recommended public and private-sector cybersecurity assessment methods.

- **Training.** In 2023, EPA is offering training for states and water systems on evaluating cybersecurity in sanitary surveys and implementing cybersecurity best practices. For states, EPA is providing in-person and remote training in each EPA Region. For water systems, EPA is delivering a series of national topic-specific webinars.
- **Technical Assistance.** Under EPA's *Cybersecurity Technical Assistance Program for the Water Sector*, water systems and states can submit questions or consult with a subject matter expert regarding water system cybersecurity, such as identifying whether a cybersecurity gap should be considered a significant deficiency or selecting appropriate risk mitigation actions. EPA's *Water Sector Cybersecurity Evaluation Program* carries out assessments of cybersecurity practices at water systems upon request by the system. The assessment follows the CISA Cybersecurity Performance Goals. The water system receives a report that shows gaps in cybersecurity, including potential significant deficiencies, which the water system can provide to the state to review during a sanitary survey.

EPA guidance also highlights important resources for water systems from water sector partners in both the government and the private sector. Examples include:

- The *Cybersecurity Framework* from the National Institute of Standards and Technology,

- The CISA *Cyber Hygiene Services* program,
- CISA *Cybersecurity Advisors*,
- The United States Department of Agriculture Rural Development Circuit Rider program and Rural Utilities Service Water and Environmental programs that provide loans, grants, loan guarantees, and technical assistance for water systems in rural communities of 10,000 people or less,
- *Water Information Sharing and Analysis Center* (ISAC) threat and response resources,
- *Multi-State ISAC* information sharing and incident response assistance,
- *American Water Works Association* guidance and tools, and
- *National Rural Water Association* training and guidance for small water systems.

EPA notes that prior to issuing the memorandum on cybersecurity in water system sanitary surveys, the Agency engaged water sector stakeholders in multiple venues to solicit input on this policy approach, including with our state co-regulators and water systems and associations. EPA derived valuable insight from these engagements, which the Agency has incorporated into the memorandum and guidance.

Moving forward, EPA will continue our work with our public and private sector partners to help water and wastewater systems become more secure and resilient against both natural hazards and malevolent acts, including the threat of cyber-attacks. These efforts remain an essential component of EPA's mission to protect public health and the environment.

Thank you for the opportunity to testify before you today, and I look forward to our discussion.