January 25, 2023

Mr. Michael Regan
Administrator
Environmental Protection Agency
1200 Pennsylvania Ave, NW
Washington, DC 20460

Re: Pending EO 12866 Regulatory Review: Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity

Dear Administrator Regan,

The undersigned associations write you regarding EPA's Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity, which OMB is currently reviewing.

Collectively we are dedicated to protecting public health and the environment by providing safe drinking water and excellent wastewater services. The infrastructure our members maintain is the foundation on which U.S. communities are built.

Cybersecurity is mission-critical for all types of water utilities. As such, we support efforts to strengthen cybersecurity, and are eager to collaborate with the agency to develop and implement effective approaches. However, EPA's planned efforts to add cybersecurity requirements to the Sanitary Survey Program for drinking water utilities are ill-advised, impractical, and are not designed to meaningfully improve system resiliency. EPA's approach is also legally flawed as described in the addendum to this letter.

We write to raise the significant legal, procedural, and policy concerns drinking water utilities have regarding the imposition of cybersecurity requirements through the Sanitary Survey

Program and offer a process to examine alternatives. Ultimately, we fear the Sanitary Survey approach could do more harm than good for drinking water utilities.

To that end, we are committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. We recognize the necessity to act, and we are committed to working expediently to develop and implement cybersecurity solutions for the water sector that are developed by consensus with critical input and support from water utilities, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector.

Thus, to best serve our shared goal of cybersecurity solutions for the water sector, we urge you to recall the RIN 2040-ZA41 Memorandum under review at the Office of Management and Budget for reconsideration with stakeholders and to ensure compliance with all applicable laws.

Sincerely,

American Water Works Association
Association of Metropolitan Water Agencies
National Association of Clean Water Agencies
National Association of Counties
National Association of Water Companies
National League of Cities
National Rural Water Association
US Conference of Mayors
Water Environment Federation

cc: Christopher Inglis – EOP/ONCD
Elizabeth Sherwood-Randall – EOP/ONSA/OHSA
Richard Revesz – EOP/OMB/OIRA
Janet McCabe – EPA/AO
Radhika Fox – EPA/OW
Jeffrey Prieto – EPA/OGC
Sean O'Donnell – EPA/OIG
Tim Del Monico – EPA/AO/OCIR
Victoria Arroyo – EPA/AO/OP

Addendum to Joint Association Letter regarding the Pending EO 12866 Regulatory Review: Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity

Statutory & Regulatory History

With increasingly severe cyber threats over the last decade, support has grown at all levels of government and within the sector to enhance water and wastewater system security and resilience. In recent years, the prevailing—and appropriate—trend was a collaborative approach to improving water and wastewater sector-specific cybersecurity through risk and resilience assessments and emergency response planning undertaken by utilities, which Congress has fully endorsed. But within that past eighteen months, EPA has made a significant shift by instead proposing regulation for drinking water utilities through the Sanitary Survey Program, an admittedly "creative"[1] approach, which we find neither practical nor legally supportable. A brief statutory and regulatory history follows:

America's Water Infrastructure Act of 2018 (AWIA)

The AWIA (PL 115-270) was passed to improve drinking water and water quality, increase water and wastewater infrastructure investments and jobs, and enhance public health and quality of life. It included significant changes to the Safe Drinking Water Act (SDWA). Among those, AWIA Section 2013 references cybersecurity in addressing community water system risk and resilience. Particularly, this section amended SDWA Section 1433 to require each community water system serving a population of greater than 3,300 persons to conduct a system risk and resilience assessment at least every five years, including the risk from malevolent acts that could "substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water", which encompasses cyber threats. SDWA § 1433(a). Further, Section 2013 requires such systems to incorporate the findings of their assessment into an emergency response plan, which includes "strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system." SDWA § 1433(b). Thus, Congress specifically highlighted cybersecurity as an issue to address through risk and resilience assessments and emergency response planning.

We would also like to call attention to the provision pertaining to alternative preparedness and operational resilience programs. SDWA § 1433(f). Specifically, consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995, this provision requires EPA to recognize voluntary consensus standards and guidance developed by third-party organizations, like AWWA, that support and facilitate the implementation of the above requirements. For example, AWWA's Cyber Security Assessment Tool and Guidance was developed in collaboration with the National Institute of Standards and Technology (NIST), the Cybersecurity

[1] Statement of Anne Neuberger, Transcript: Securing Cyberspace, The Washington Post (Oct. 13, 2022), https://www.washingtonpost.com/washington-post-live/2022/10/13/transcript-securing-cyberspace/.

and Infrastructure Security Agency (CISA), and EPA representatives in 2014 (and updated in 2019) to provide a consensus-based, sector-specific approach to the NIST cybersecurity framework. Yet, EPA has not leveraged this option to advance the agencies mission in support of AWIA §2013 and related cybersecurity objectives.

Infrastructure Investment & Jobs Act of 2021

A significant component of the Infrastructure Investment and Jobs Act (PL 117-58) was greater investment and support to rehabilitate and update water infrastructure, including through several authorizations that support cybersecurity improvements. For example, the Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program (sec. 50107) and the Clean Water Infrastructure Resilience and Sustainability Program (sec. 50205) provide grant funding from EPA to help reduce cybersecurity vulnerabilities, among other priorities, at drinking water and wastewater systems. Similarly, the Act (sec. 50113) required EPA and CISA to develop and report to Congress (1) a prioritization framework to identify public drinking water systems that, if degraded or rendered inoperable, would have significant public health and safety impacts, taking into consideration any identified cybersecurity vulnerabilities and independent capacity to address such vulnerabilities, and (2) a technical cybersecurity support plan for public drinking water systems with a methodology for identifying for which systems cybersecurity support should be priorities, timelines for making voluntary technical support available, and specific capabilities that could be utilized to provide such support. These were completed in May 2022[2] and August 2022[3], respectively. Congress did not, however, authorize EPA to develop or otherwise impose cybersecurity requirements on water utilities.

EPA Unified Agenda – Fall 2021[4]

In the Fall 2021 Unified Agenda listed EPA/OW RIN 2040-AG20, Cybersecurity in Public Water Systems, as a rulemaking in the final rule stage. EPA indicated that it was evaluating regulatory approaches to improve cybersecurity at public drinking water systems. While EPA planned to offer separate guidance, training, and technical assistance to states and public drinking water systems on cybersecurity, EPA also announced its plan to issue this Final Interpretive Rule to "provide regulatory clarity and certainty and promote the adoption of cybersecurity measures by public water systems." Particularly, EPA proposed to include cybersecurity assessments as part of the regular drinking water Sanitary Survey Program:

> Sanitary surveys, which states, tribes, or the EPA typically conduct every 3 to 5 years on all public water systems, should include an evaluation of cybersecurity to identify significant deficiencies. EPA recognizes, however, that many states

[2] https://www.epa.gov/system/files/documents/2022-08/Prioritization%20Framework%20RtC%20final.pdf

[3] https://www.epa.gov/system/files/documents/2022-08/9910_RtC-Technical%20Cybersecurity%20Support%20Plan_20220818_final.pdf

[4] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=2040-AG20

> currently do not assess cybersecurity practices during public water system sanitary surveys. This action is necessary to convey to states that EPA interprets existing regulations for public water system sanitary surveys as including the possible identification of significant deficiencies in cybersecurity practices.

EPA justified the interpretive rule under the Administrative Procedure Act ("APA") as an "interpretation of existing responsibilities under current regulations" stating that "[i]t establishes no new regulatory requirements and, hence, has no regulatory costs or benefits." Importantly, EPA explicitly acknowledged that there were alternatives to the interpretive rule approach, specifically that EPA could "[p]rovide guidance to states, tribes, and EPA on evaluating cybersecurity practices during public water system sanitary surveys without issuing an interpretive rule."

EPA said it would issue a Final Interpretive Rule in April 2022. However, in response to this proposal, in December 2021, water system associations asked EPA to not pursue this regulatory strategy, citing various significant concerns with its legality under the APA, inadequate protection of sensitive information, lack of national consistency given that the Sanitary Survey Program is implemented by states, insufficient skill and training of state staff. (*e.g.*, AWWA 12/9/21 letter, Association of State Drinking Water Administrators 9/29/21, 2/9/22, 11/21/22 letters).

EPA Unified Agenda – Spring 2022[5]

Following these public comments, EPA recategorized EPA/OW RIN 2040-AG20, Cybersecurity in Public Water Systems, as a "Long-Term Action" in the Spring 2022 Unified Agenda. Additionally, in a May 2022 budget hearing before the House Committee on Energy and Commerce's Subcommittee on Environment and Climate Change, EPA assured the subcommittee that the Agency would be transparent in its rulemaking processes to allow for proper public notice and comment. Further, when asked about water and wastewater cybersecurity, the Agency indicated that it is "laser focused on this cybersecurity issue" and "using all of our statutory authority to pursue cybersecurity in the water space that we can." Stating further that EPA would not outsource its leadership responsibility in the water and wastewater cybersecurity space, engage regularly with the water sector and the Coordinating Council on Cybersecurity. The Agency committed to making each of these assurances in writing; however, to our knowledge, those written assurances have not been made. The Fiscal Year 2023 EPA Budget, Houston of Representatives, Subcommittee on Environment and Climate Change, Committee on Energy and Commerce, Washington, D.C. (May 17, 2022) at 1737-1837.

EPA Unified Agenda – Fall 2022[6]

The most recent Unified Agenda retitled the "Long Term Action" for EPA/OW RIN 2040-AG20 to "Public Water System Cybersecurity Requirements." This action is summarized

[5] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=2040-AG20

[6] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=2040-AG20

as "evaluating regulatory approaches to improve cybersecurity at public water systems. EPA plans to offer separate guidance, training, and technical assistance to states and public water systems on cybersecurity. This action will provide regulatory clarity and promote the adoption of cybersecurity measures by public water systems."

OMB/OIRA RIN 2040-ZA41 – Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity

On December 16, 2022, EPA submitted RIN: 2040-ZA41, *Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity*, to OMB/OIRA for review. While EPA has not made the memo or its contents public, we suspect it is substantively the same as the prior proposed interpretive rule. Accordingly, AWWA, AMWA, NRWA, NAWC, WEF, and NACWA requested a meeting with OMB to discuss the memo and express our concerns with a Sanitary Survey Program-based approach.

We are also aware that the Association of State Drinking Water Administrators (ASDWA) had a meeting with OMB expressing similar concerns with the prospective imposition of regulatory burden resulting from this Memo. In addition, concerns were also expressed by AWWA about the Memo and EPA's process during the public comment period of the January 13, 2023, meeting of EPA's Local Government Advisory Committee.

Response and Recommendations

While we appreciate that EPA has moved from a Final Interpretive Rule to Long-Term Action, and while the contents of the RIN: 2040-ZA41 memorandum are not yet public, we have significant concerns that EPA has yet to address. Proceeding at this stage with any sort of regulatory requirement would be premature.

First, as explained in a December 9, 2021, letter from AWWA, AMWA, NAWC, and NRWA to Assistant Administrator of Water Radhika Fox: "We do not believe an agency action to establish cybersecurity requirements through an interpretive rule is legally justifiable, as interpretive rules must not set new legal standards or impose new requirements." If the effect of EPA's action is still to impose cybersecurity requirements on operators at public drinking water systems, EPA must satisfy the APA and other legal prerequisites, or may otherwise be subject to judicial review. 5 U.S.C. § 706(2)(A); *Mortg. Bankers Ass'n. v. Harris*, 720 F.3d 966 (D.C. Cir. 2013) (quoting *F.C.C. v. Fox Television Stations*, 556 U.S. 502, 513 (2009) for the holding that the APA provides the full scope of "judicial authority to review executive agency action for procedural correctness.").

An interpretive rule "simply indicates an agency's reading of a statute or a rule. It does not intend to create new rights or duties, but only reminds affected parties of existing duties." *Paralyzed Veterans of Am. V. West*, 138 F.3d 1434 (Fed. Cir. 1994) (quoting *Orengo Caraballo v. Reich*, 11 F.3d 186, 195 (D.C.Cir.1993)). "The critical feature of interpretive rules is that they are

issued by an agency to advise the public of the agency's construction of the statutes and rules which it administers." *Perez v. Mortgage Bankers Ass'n*, —— U.S. ——, 135 S.Ct. 1199, 1204, 191 L.Ed.2d 186 (2015) (citation omitted). "The most important factor in differentiating between binding and nonbinding actions is "the actual legal effect (or lack thereof) of the agency action in question. . . Agency action that creates new rights or imposes new obligations on regulated parties or narrowly limits administrative discretion constitutes a legislative rule." *Ass'n of Flight Attendants-CWA, AFL-CIO v. Huerta*, 785 F.3d 710, 717 (D.C. Cir. 2015) (citing *Nat'l Mining Ass'n v. McCarthy*, 758 F.3d 243, 252 (D.C.Cir.2014). The hallmark of an interpretive rule is that such rules are exempt under the APA from public notice and comment requirements. 5 U.S.C. § 553(b)(A). However, when a rule goes beyond that advisory or confirmatory purpose, it is considered a legislative rule, to which public notice and comment requirements apply. 5 U.S.C. § 553(b).

EPA's Memo to add cybersecurity requirements to the Sanitary Survey Program goes well beyond merely providing the "regulatory clarity and certainty" it purports, and does, in fact, establish new regulatory requirements not otherwise imposed under the SDWA. The Sanitary Survey Program is a precondition of state primacy, which is a "systematic program for conducting sanitary surveys of public water systems in the State," which includes an "onsite review of the water source (identifying sources of contamination using results of source water assessments where available), facilities, equipment, operation, maintenance, and monitoring compliance of a public water system to evaluate the adequacy of the system, its sources and operations and the distribution of safe drinking water." SDWA § 1413; 40 C.F.R. §§ 142.10, 142.16. EPA's Memo would seek to add cybersecurity to the state primacy requirements. Although the Sanitary Survey Program requirements generally cover operations, they have never included cybersecurity nor was the Program drafted with cybersecurity in mind — yet EPA is now attempting to tenuously read it in. Such an action would constitute an entirely new requirement, going well beyond the purpose of an interpretive rule. Moreover, SDWA Section 1433 requires that certain drinking water systems conduct risk and resilience assessments that include cybersecurity considerations, then incorporate the assessment findings into an emergency response plan with particulars on how resilience can be improved and implementation of such procedures. It does not, however, require that cybersecurity be part of the state Sanitary Survey Program or be enforced as such. EPA's proposed actions therefore are also inconsistent with Congressional intent.

In addition to this noncompliance with the APA, EPA has not held any open stakeholder engagement on its Final Interpretive Rule or as part of development of the RIN 2040-ZA41 Memorandum, nor has it held a cooperative federalism or Unfunded Mandates Reform Act (2 U.S.C. § 1501 et seq.) consultation with representatives of local and state government. Essentially, EPA has proceeded despite ample opposition from multiple water and wastewater organizations, including state administrators, and without sufficiently engaging with those most affected despite offering assurances to Congressional leaders that such engagements would take place.

More importantly, EPA's proposal to include cybersecurity requirements within the drinking water Sanitary Survey Program administered by state sanitarians is a sub-optimal way to address cybersecurity challenges posed to critical water infrastructure systems. As repeatedly noted by the ASDWA (9/29/21, 2/9/22, 11/21/22 Letters), for example, state authorities that administer the Sanitary Survey Program lack the appropriate staffing, training and expertise to evaluate cybersecurity programs. Even with training, given the complexity of cybersecurity

measures and their relatively rapid evolution, agency staff could misunderstand best practices and their implementation, resulting in an unmerited deficiency or a redirection from a practice that is sufficiently securing the utility. Nothing in federal or state law protects information collected through state agencies' sanitary surveys from being shared publicly, and such disclosures could risk exposing system vulnerabilities to actors who pose cybersecurity threats.

To address these issues and concerns we are committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. We recognize the necessity to act, and we are committed to working expediently to develop and implement cybersecurity solutions for the water sector that are developed by consensus with critical input and support from water utilities, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector.

Thus, to best serve our shared goal of cybersecurity solutions for the water sector, we urge you to recall the RIN 2040-ZA41 Memorandum under review at the Office of Management and Budget for reconsideration with stakeholders and to ensure compliance with all applicable laws.