

No. 23-1787

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATES OF MISSOURI, ARKANSAS, IOWA,
Petitioners,

v.

MICHAEL REGAN, IN HIS OFFICIAL CAPACITY AS ADMINISTRATOR OF THE U.S.
ENVIRONMENTAL PROTECTION AGENCY; U.S. ENVIRONMENTAL PROTECTION
AGENCY, AND RADHIKA FOX, IN HER OFFICIAL CAPACITY AS ASSISTANT
ADMINISTRATOR OF THE U.S. ENVIRONMENTAL PROTECTION AGENCY,
Respondents.

On Petition for Review of Final Action by the
United States Environmental Protection Agency

**PETITIONERS-INTERVENORS AMERICAN WATER WORKS
ASSOCIATION'S AND NATIONAL RURAL WATER ASSOCIATION'S
MOTION FOR STAY PENDING REVIEW**

Corinne V. Snow
Vinson & Elkins LLP
1114 Avenue of the Americas
32nd Floor
New York, NY 10036
Phone: (212) 237-0157
Email: csnow@velaw.com

*Counsel for Intervenors American
Water Works Association and
National Rural Water Association*

Dated: June 12, 2023

INTRODUCTION

Over the concerns of public water systems (“PWSs”) and several states, the Environmental Protection Agency (“EPA”) issued an immediately effective rule imposing new requirements to address cybersecurity at PWSs under the Safe Drinking Water Act (“SDWA”) and its implementing regulations. EPA issued this rule, “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process” (“Cybersecurity Rule” or “Rule”), *see* A.R. Doc. 1, without notice and comment under the Administrative Procedure Act (“APA”) and without authority under the SDWA. This legally deficient Rule poses substantial, irreparable harm to Petitioners-Intervenors American Water Works Association’s and the National Rural Water Association’s (collectively, “Associations”) PWS members.

The clock is already ticking: PWSs are presently forced to begin expending resources to amend their cybersecurity systems to comply with the Cybersecurity Rule or risk enforcement actions or other serious consequences. Some members are already scheduled to be surveyed (audited) for compliance before this case’s resolution—particularly in light of the new briefing schedule. These costs will strain the limited budgets of many members, and be passed on to the public in the form of higher drinking water rates.

Associations are likely to succeed on the merits of their claims because the Rule is procedurally deficient under the APA and exceeds EPA’s authority under the

SDWA by (1) attempting to use an existing regulatory scheme that has never contemplated cybersecurity at PWSs and (2) ignoring the existing congressional scheme to address cybersecurity concerns.

Associations respectfully request the Court stay the Cybersecurity Rule pending its review pursuant to Federal Rule of Appellate Procedure 18(a)(2) and the APA, 5 U.S.C. § 705. State Petitioners¹ support this motion; EPA denied Associations' request for a voluntary stay of the Rule and opposes this motion. *See* Fed. R. App. P. 18(a)(2)(C). In light of EPA's response and the irreparable harm Associations' members face, it would be impracticable and futile to formally seek a stay from EPA. *Id.* 18(a)(2)(A)(i), (C).

BACKGROUND

I. Addressing Cybersecurity under the SDWA

Beginning in 2002 Congress has acted on concerns about cybersecurity vulnerabilities to the nation's drinking water supply. *See, e.g.*, 147 Cong. Rec. S13,902, S13,903 (Dec. 20, 2001); H.R. Rep. No. 107-298, at 326 (2001). Congress amended the SDWA to require community water systems ("CWSs")² serving more than 3,300 individuals to assess the system's vulnerability to terrorist or other

¹ Petitioners are the States of Missouri, Arkansas, and Iowa.

² CWSs are PWSs that regularly serve at least 25 individuals year-round.

intentional acts that would jeopardize the health and access of drinking water. *See* Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188, § 401, 116 Stat. 594, 682 (codified at 42 U.S.C. § 300i-2). This limitation was important, as these larger PWSs served around 50% of the population, but only made up 0.002% of all systems. *See* Mary Tiemann, Cong. Rsch. Serv., RL31294, *Safeguarding the Nation’s Drinking Water: EPA and Congressional Actions 1* (2002).

These amendments broadly “require[d] a comprehensive review of the ways to detect and respond to chemical, biological, radiological contamination of drinking water, as well as ways to prevent and mitigate the effects of physical attacks upon those assets.” 148 Cong. Rec. H638-39 (Feb. 28, 2002) (statement of Rep. Tauzin). For CWSs serving fewer than 3,300 people, Congress directed EPA to provide guidance on how to conduct vulnerability assessments, prepare emergency response plans (“ERP”), and address threats. *See* 42 U.S.C. § 300i-2(d) (2004).

In 2018, Congress passed America’s Water Infrastructure Act (“AWIA”), modifying § 1433 to “updat[e] antiterrorism and resilience measures at public water systems.” H.R. Rep. No. 115-1126, at 77 (2019); *see* AWIA, Pub. L. No. 115-270. AWIA expanded the risks CWSs should evaluate and mandated that they update their assessments and ERPs. *See* 42 U.S.C. § 300i-2. AWIA also identified

cybersecurity as part of resilience strategies in ERPs and removed the requirement that CWSs submit their assessments to EPA. *See id.*

II. Sanitary Surveys

In contrast to § 1433’s statutory requirements, sanitary surveys are regulatory tools EPA developed in the 1970s to implement and enforce health-based drinking water standards, called National Primary Drinking Water Regulations. Sanitary surveys review the “water source, facilities, equipment, operation, and maintenance of a [PWS] for the purpose of evaluating the adequacy of such source, facilities, equipment, operation, and maintenance for producing and distributing safe drinking water.” 40 C.F.R. §§ 141.2, 142.16(b)(3). States must conduct periodic sanitary surveys for certain PWSs in order to secure and retain primary enforcement authority under the SDWA. *See id.* § 142.16(b), (o). If states identify a “significant deficiency”³ during a survey, they must require PWSs to address the deficiency. *Id.* § 142.16(b)(1)-(3), (o)(1)-(2). Before the Rule, many, if not all states, did not review cybersecurity practices during sanitary surveys. *See* A.R. Doc. 50 at 4; Mot. to Intervene, Ex. A, Decl. of G. Tracy Mehan, III (“AWWA Decl.”) ¶49; Ex. B,

³ Significant deficiencies are “defects in design, operation, or maintenance, or a failure or malfunction of the sources, treatment, storage, or distribution system that the State determines to be causing, or have potential for causing, the introduction of contamination into the water delivered to consumers.” 40 C.F.R. § 142.16(o)(2)(iv).

Decl. of Matthew Holmes (“NRWA Decl.”) ¶44. Indeed, “[s]tates [d]id not have authority to require water utilities to conduct cybersecurity vulnerability assessments and develop risk mitigation plans [and] would be required to establish new regulations.” A.R. Doc. 50 at 4.

III. EPA’s Cybersecurity Rule

The Rule requires states to “evaluate the cybersecurity of operational technology used by a PWS when conducting PWS sanitary surveys or through other state programs.” A.R. Doc. 1 at 1. To comply, states must “evaluate the adequacy of the cybersecurity of that operational technology for producing and distributing safe drinking water”; and “[i]f the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency.” *Id.* at 2-3. A guidance document accompanying the Rule includes a thirty-six item checklist of cybersecurity controls that states should look for and evaluate during sanitary surveys and characterizes the absence or inadequacy of sixteen of these controls to be potential “significant deficiencies,” thereby exposing PWSs to enforcement risk. *See* A.R. Doc. 2 at 11-14 and App. A.

ARGUMENT

This Court considers four factors in determining whether to stay agency action pending review: (1) likelihood of success on the merits; (2) irreparable harm to the

movant absent a stay; (3) balance of harms among other parties interested in the proceeding; and (4) whether a stay would serve the public interest. *Nken v. Holder*, 556 U.S. 418, 434 (2009) (citation omitted); see *Brady v. Nat'l Football League*, 640 F.3d 785, 789 (8th Cir. 2011).

I. Associations Have a Fair Chance of Prevailing on the Merits.

“Likelihood of success on the merits is the most important factor, and requires a movant to demonstrate at least a ‘fair chance of prevailing.’” *Wildhawk Invs., LLC v. Brava I.P., LLC*, 27 F.4th 587, 593 (8th Cir. 2022) (citations omitted). This Court sets aside EPA actions that are “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law”; “in excess of statutory jurisdiction, authority, or limitations”; or “without observance of procedure required by law.” 5 U.S.C. § 706(2)(A), (C)-(D); see *Northport Health Servs. of Ark., LLC v. Dep’t of Health & Human Servs.*, 14 F.4th 856 (8th Cir. 2021).

Associations have a fair chance of prevailing in their claims that (1) EPA unlawfully issued the Cybersecurity Rule without observing the APA’s notice-and-comment requirements; (2) the Rule exceeds EPA’s authority under the SDWA; and (3) the Rule is arbitrary and capricious.⁴

⁴ While the fair-chance standard applies “in most instances,” this Court has applied a heightened “likely to prevail” standard where a movant challenges “government action based on presumptively reasoned democratic processes.” *D.M. by Bao Xiong v. Minn. State High Sch. League*, 917 F.3d 994, 999-1000 (8th Cir. 2019) (citations

A. The Cybersecurity Rule is a legislative rule published in violation of the APA.

EPA did not follow the APA's notice-and-comment procedures applicable to legislative rules. *See* 5 U.S.C. § 553(b)(1)-(3), (c). Because the Rule *is* a legislative rule that “imposes new rights or duties,” its issuance was unlawful. *Iowa League of Cities v. EPA*, 711 F.3d 844, 873 (8th Cir. 2013) (quoting *Nw. Nat'l Bank v. U.S. Dep't of the Treasury*, 917 F.2d 1111, 1117 (8th Cir. 1990)), *enforced*, No. 11-3412, 2021 WL 6102534 (8th Cir. Dec. 22, 2021).

First, the Rule's requirements are new and materially differ from the traditional focus of sanitary surveys as described by EPA's regulations and prior guidance. There is therefore no “external legal basis” for the Rule, *Iowa League of Cities*, 711 F.3d at 874, nor does the Rule “remind affected parties of existing

omitted). The likely-to-prevail standard applies where there has been “lengthy public debate involving both the legislative and executive branches before the formulation of the [action] and its subsequent enactment.” *Id.* at 1000. District courts have applied the standard where an agency “engaged in the requisite notice and comment period,” such as pursuant to the APA or state analogue. *See, e.g., First Premier Bank v. CFPB*, 819 F. Supp. 2d 906, 911, 913 (D.S.D. 2011); *Aventure Commc'n Tech., LLC v. Iowa Utils. Bd.*, 734 F. Supp. 2d 636, 655 (N.D. Iowa 2010).

While Associations would meet either standard, the less rigorous, fair-chance standard applies here because EPA unilaterally issued the Cybersecurity Rule without formal public notice and comment, unlike the agency rules in *First Premier* and *Aventure*, and without meaningful external debate. *See also Richland/Wilkin Joint Powers Auth. v. U.S. Army Corps of Eng'rs*, 826 F.3d 1030, 1040-41 (8th Cir. 2016) (fair-chance standard applied) (internal quotation marks omitted).

duties,” *Nw. Nat’l Bank*, 917 F.2d at 1117 (internal quotation marks omitted). *See Catholic Health Initiatives v. Sebelius*, 617 F.3d 490, 494 (D.C. Cir. 2010) (interpretive rules must “derive . . . from an existing document whose meaning compels or logically justifies the proposition”) (internal quotation marks omitted). EPA’s existing sanitary survey regulations are silent as to cybersecurity. *See* 40 C.F.R. § 142.16(b)(3), (o)(1)-(2). EPA contends that its regulations’ use of “operation” and “equipment” to define the scope of sanitary surveys captures the cybersecurity of PWSs’ operational technology. *See id.*; A.R. Doc. 1 at 2-3 & n.14. But EPA’s most recent substantive revisions to its sanitary survey requirements do not mention cybersecurity, much less how cybersecurity is captured by “operation” or “equipment.” *See* National Primary Drinking Water Regulations: Ground Water Rule, 71 Fed. Reg. 65,574 (Nov. 8, 2006); National Primary Drinking Water Regulations: Interim Enhanced Surface Water Treatment, 63 Fed. Reg. 69,478 (Dec. 16, 1998).

Similarly, EPA’s prior guidance regarding the scope of sanitary survey programs recognizes PWSs’ use of remote signaling or operation systems, sometimes referred to as SCADA systems, are notably silent on states’ need to assess the *cybersecurity* of those systems. Those guidance documents, spanning hundreds of pages, do not mention the type of cybersecurity considerations for PWSs’ remote systems contained in the Cybersecurity Rule and associated guidance (e.g.,

passwords, credentials, network configurations, software, vendors' cybersecurity). Instead, the documents highlight potential significant deficiencies that relate to the installation, operations, maintenance, and training for remote systems. *See* A.R. Doc. 11 (EPA's August 2019 guidance) at 5-18 to 5-19, 10-8 (security focused on physical aspects such as "fencing and gates; lights; locks on hatches, ladders, vaults, and buildings; intrusion alarms; and cameras"), 13-9, 15-5; A.R. Doc. 61 (EPA's October 2008 guidance) at 4-74 to 4-75. Those considerations are totally distinct from cybersecurity.

EPA cannot now "announc[e]" a "specif[ic] applicat[i]o[n]" of otherwise "vague or vacuous terms" to impose new legislative requirements while also avoiding notice and comment. *Catholic Health*, 617 F.3d at 494-95 (citation omitted); *accord Mendoza v. Perez*, 754 F.3d 1002, 1015, 1020-21 (D.C. Cir. 2014); *Hoctor v. U.S. Dep't of Agric.*, 82 F.3d 165, 167-70 (7th Cir. 1996). Likewise, EPA cannot shoehorn cybersecurity into terms like "operation" and "equipment" to bypass the APA and impose cybersecurity audit requirements, about which EPA's regulations and guidance have not previously provided notice.

Second, the Cybersecurity Rule is "quintessentially legislative." Rather than simply interpreting, EPA is "identifying a practical problem" and "put[ting] forward a new and different resolution." *Nat. Res. Def. Council v. Wheeler*, 955 F.3d 68, 83 (D.C. Cir. 2020) ("*NRDC*"). EPA details the need for cybersecurity audits, including

PWSs’ “increasing[] reli[ance] on the use of electronic systems to operate drinking water systems efficiently” and instances of “[m]alicious cyber activity incidents . . . impact[ing] PWSs’ ability to deliver safe drinking water.” A.R. Doc. 1 at 2, 8. EPA further highlights countervailing considerations (e.g., relative inexperience of state regulators in auditing cybersecurity systems, risk of public disclosure of PWSs’ cybersecurity information), and proposes several options for states to meet their new mandate (e.g., state sanitary surveys, PWS self-assessments, third-party assessment). *See id.* at 3-7, 11-12. No matter the label EPA affixes, the Cybersecurity Rule is an exercise of EPA’s legislative function—identifying a problem, weighing costs and benefits of solutions, and selecting a solution to implement. The Rule, by its nature, is legislative. *See NRDC*, 955 F.3d at 83; *see also Hoctor*, 82 F.3d at 167-70 (“cho[osing] among methods of implementation” is a legislative act).

Third, the Cybersecurity Rule’s requirements are binding. The Rule mandates that states—the many if not all of which did not previously review cybersecurity practices during sanitary surveys—“must evaluate the adequacy of the cybersecurity of [a PWS’s] operational technology,” as part of their sanitary survey programs and “must use [their] authority to require [a] PWS to address [a] significant deficiency” identified during a survey. A.R. Doc. 1 at 2-3; *see also* AWWA Decl. ¶49; NRWA Decl. ¶44. Through repeated use of “must,” EPA binds states, obligating them to incorporate cybersecurity audits into sanitary surveys. Additionally, the Rule directs

states to take a particular action (i.e., order mitigation) whenever a given event arises (i.e., a cybersecurity-related significant deficiency is identified during an audit). It thus mandates State enforcement. *See Kisor v. Wilkie*, 139 S. Ct. 2400, 2420 (2019) (“An interpretive rule itself never forms ‘the basis for an enforcement action’ An enforcement action must instead rely on a legislative rule, which (to be valid) must go through notice and comment.”) (citations omitted) (plurality opinion).

Eliminating state discretion is indicative of a legislative rule, *see Iowa League of Cities*, 711 F.3d at 874, and stands in marked contrast to an interpretive rule, which imposes no binding obligations or prohibitions such that a regulator is “free to ignore its provisions if it so chooses,” *South Dakota v. Ubbelohde*, 330 F.3d 1014, 1028 (8th Cir. 2003); *accord Nat’l Min. Ass’n v. McCarthy*, 758 F.3d 243, 251-52 (D.C. Cir. 2014). Similarly, the Rule’s requirement that states sanction PWSs, such as through “follow-on risk mitigation plans” with “list[ed] planned mitigation actions and schedules” and continuing state review, A.R. Doc. 1 at 3-4, has the legal effect of requiring PWSs to adjust their conduct. *Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 21 n.8 (D.C. Cir. 2006).

B. Even if the Rule was interpretive, EPA exceeded its authority under the SDWA.

EPA’s power to act and how it acts is “authoritatively prescribed by Congress.” *City of Arlington v. FCC*, 569 U.S. 290, 297 (2013). “An agency’s

promulgation of rules without valid statutory authority implicates core notions of the separation of powers, and [this Court is] required by Congress to set these regulations aside.” *U.S. ex rel. O’Keefe v. McDonnell Douglas Corp.*, 132 F.3d 1252, 1257 (8th Cir. 1998) (citing 5 U.S.C. § 706(2)(C)). EPA exceeded its authority under the SDWA in issuing the Cybersecurity Rule.

First, § 1433 already prescribes a scheme requiring larger CWSs to assess their cybersecurity risks, periodically review and revise the assessment, and develop ERPs that must include strategies and procedures to improve their cybersecurity. 42 U.S.C. § 300i-2(a)-(b). In this scheme, EPA plays a passive role, receiving certifications that CWSs completed their AIWA requirements, *id.* § 300i-2(a)(3), and providing agencies “baseline information on malevolent acts of relevance to community water systems” and “guidance and technical assistance” to smaller CWSs on conducting resilience assessments, preparing ERPs, and addressing threats. *Id.* § 300i-2(a)(2), (e).

While these provisions task EPA with providing information about cybersecurity, they do not grant EPA authority to regulate the cybersecurity practices of CWSs, nor do they require that cybersecurity be part of sanitary surveys. CWSs must submit to EPA certifications of their completed risk and resilience assessments, but these certifications “shall contain *only*” information that identifies the CWS, the date of certification, and a statement that the system has conducted, reviewed, or

revised the assessment. *Id.* § 300i-2(a)(4) (emphasis added). Nowhere in the SDWA does Congress grant EPA any authority to regulate, or compel states to regulate, the cybersecurity practices of CWSs. *See* 148 Cong. Rec. H2844-45 (May 22, 2002) (statement of Rep. Tauzin) (“No new authorities were transferred to the [EPA] beyond the passive receipt of vulnerability assessments under Section 1433.”); *id.* H2851-52 (statement of Rep. Gillmor) (“EPA is not given any rulemaking or other authority to define further what is or is not a vulnerability assessment meeting the requirements of section 1433.”). As EPA confirmed in the Rule, § 1433 “does not provide for any review of the risk and resilience assessments by states, nor does it require water systems to adopt specific cybersecurity practices to reduce risks identified during the risk and resilience assessments.” A.R. Doc. 1 at 9.

Second, the Cybersecurity Rule exceeds EPA’s statutory authority because it applies *more* requirements to *all* PWSs, whereas Congress intended to apply *limited* requirements to *a subset of* PWSs. Since § 1433’s enactment, *only* those CWSs serving populations over 3,300 are required to conduct risk assessments and complete ERPs. Smaller PWSs have always been exempt because they have limited budgets, operational capacities, and customer bases. *See* H.R. Rep. No. 115-380, at 12 (2017) (“82 percent of all CWSs[] are relatively small, serving 3,300 people or fewer; but these systems provide water to just 9 percent of the total population served

by community water systems. In contrast, 8 percent of all CWSs serve 82 percent of the population served.”).

The Rule thus defies Congress’s preference that § 1433 should only impose cybersecurity-related obligations on the minority of systems that serve a majority of the population. For smaller systems, Congress instead required EPA to “provide guidance and technical assistance to” these CWSs. 42 U.S.C. § 300i-2(e). By subjecting smaller PWSs to these new sanitary survey requirements and compelling them to expend their limited budgets on analyzing and complying with the Rule, *see* NRWA Decl. ¶10; Mot. to Intervene, Ex. F, Decl. of Frank Dennis Offutt (“Offutt Decl.”) ¶28, the Rule contravenes the scheme Congress devised to address this issue.

Third, § 1433 repeatedly safeguards collection of sensitive cybersecurity information. The legislative history reflects Congress’s concern that information contained in such assessments would be disclosed to and weaponized by unauthorized or bad actors. *See* 148 Cong. Rec. H2844-45 (May 22, 2002) (statement of Rep. Tauzin). By requiring that states evaluate this information as part of periodic sanitary surveys of PWSs, the Cybersecurity Rule necessarily requires states to collect sensitive cybersecurity information. CWSs lack control or assurance of security of this information, *see* Mot. to Intervene, Ex. G, Decl. of Scott Borman (“Borman Decl.”) ¶34, and if a state finds a significant deficiency related to cybersecurity controls, such findings may be made publicly available, placing PWSs

at further risk of harm. *See id.*, Ex. I, Decl. of John R. Dunn (“Dunn Decl.”) ¶12; A.R. Doc. 50 at 5 (“States have significant concerns with public disclosure of sensitive information when identifying and resolving violations related to cybersecurity.”). These are consequences Congress sought to prevent when enacting § 1433.

For the same reasons, the Rule violates the APA. Courts set aside agency actions that are “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C. § 706(2)(A). This standard requires agencies to act with reasoned judgment and provide a “rational connection between the facts found and the choice made.” *Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). Here, EPA “relied on factors which Congress has not intended it to consider [or] entirely failed to consider an important aspect of the problem” and failed to provide a reasoned explanation for its new interpretation of a “sanitary survey,” relied on an authority that Congress did not intend to give, and failed to consider states’ resources and experience, as well as their inability to safeguard this sensitive information. *Id.*

II. The Balancing of Harms and the Public Interest Support a Stay Pending Review.

A. Absent a stay, Associations’ members will suffer irreparable harm to their operational and financial interests.

An injury is “irreparable” if it “cannot be remedied by a later award of money damages.” *Kroupa v. Nielsen*, 731 F.3d 813, 820 (8th Cir. 2013). Monetary damages are not available relief under the APA. *See Alphapointe v. Dep’t of Veterans Affs.*, 416 F. Supp. 3d 1, 9 (D.D.C. 2019); *see also Red Lake Band of Chippewa Indians v. Barlow*, 846 F.2d 474, 476 (8th Cir. 1988) (APA waiver of sovereign immunity “dependent on the suit against the government being one for non-monetary relief”). Absent a stay, Associations’ members face two injurious scenarios: One, expend unrecoverable time and resources to alter their cybersecurity systems to comply with the cybersecurity controls specified by EPA, and/or unnecessarily charge customers for the costs even if the Cybersecurity Rule is later vacated. Or two, risk a finding of significant deficiency for failing to implement a particular cybersecurity control and incur the associated monetary, operational, and reputational harms. Neither harm is reparable, and under the present briefing schedule, members will face surveys before this case is resolved. *See, e.g.,* Dunn Decl. ¶11 (survey scheduled for Fall 2023).

Many PWSs have limited budgets and must pass costs on to customers in the form of higher rates. Mot. to Intervene, Ex. D, Decl. of Robert J. Walters (“Walters

Decl.”) ¶28. PWSs’ implementation of the Rule will require significant expenditures, extensive coordination, and long lead-times for budgeting, procurement, planning, and implementation.⁵ *See, e.g.*, Mot. to Intervene, Ex. E, Decl. of Cynthia Lane (“Lane Decl.”), ¶¶19, 20, 24 (estimating system’s information technology budget “will need to be doubled, at the very least[,]” to comply with the Rule); Offutt Decl. ¶¶17-19, 29; Borman Decl. ¶¶20-21, 25 (estimating an additional “\$75,000 to \$100,000” to the system’s fiscal year 2024 budget will be necessary). These costs are compounded by PWSs’ lack of advance notice of the Rule so that they could plan, budget for, and complete any necessary work. This is especially true for Associations’ members with upcoming sanitary surveys. *See* Dunn Decl. ¶11.

Although the magnitude of these harms is great relative to the finances of many PWSs, *see, e.g., id.* at ¶23; Lane Decl. ¶¶20, 24; Borman Decl. ¶¶20-21, the focus is “not so much the magnitude but the irreparability.” *See Enter. Int’l, Inc. v. Corporacion Estatal Petrolera Ecuatoriana*, 762 F.2d 464, 472 (5th Cir. 1985) (citation omitted). Many PWSs rely on regulated rates and/or budgetary allocations to recoup costs, with rates and appropriations linked to customer needs. *See* AWWA

⁵ One credit rating agency has already recognized that PWSs will likely incur significant costs to conform to the Cybersecurity Rule. *See* Fitch Wire, *EPA Memo Ramps Up Cyber Regulations for Water Utilities*, FitchRatings (May 11, 2023, 3:22 PM), <https://tinyurl.com/4vp8md9r>.

Decl. ¶¶28-29; NRWA Decl. ¶28; Lane Decl. ¶20; Dunn Decl. ¶¶23-24; Borman Decl. ¶3. Even if the Court finds the Cybersecurity Rule unlawful, PWSs could not recover their interim compliance costs from anyone but their customers. *See Iowa Utils. Bd. v. FCC*, 109 F.3d 418, 426 (8th Cir. 1996) (economic losses irreparable where petitioner “would not be able to bring a lawsuit to recover their undue economic losses if the [agency’s] rules are eventually overturned”); *see also Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 220-21 (1994) (Scalia, J., concurring in part and in judgment) (“[C]omplying with a regulation later held invalid almost always produces the irreparable harm of nonrecoverable compliance costs.”) (emphasis omitted).

The Cybersecurity Rule increases the risk of a finding of significant deficiency, which invites a host of irreparable financial, operational, and reputational harms. While many PWSs have cybersecurity systems tailored to operational needs, they do not necessarily have every single measure specified by EPA. *See AWWA Decl. ¶38; NRWA Decl. ¶45; Lane Decl. ¶17; Mot. to Intervene, Ex. C, Decl. of Mark Pepper (“Pepper Decl.”) ¶19; Walters Decl. ¶¶18, 22.* Thus, absent significant (and potentially unrecoverable) expenditures, the Rule increases PWSs’ enforcement risk. *See Sleep No. Corp. v. Young*, 33 F.4th 1012, 1018 (8th Cir. 2022) (movant need not “prove with certainty the threat of irreparable harm,” only that such harm “is likely in the absence of an injunction.” (citation omitted)). This is

especially true for Associations’ members with upcoming sanitary surveys before this Court renders a decision on the merits based on the current briefing schedule. *See* Dunn Decl. ¶11.

Findings of significant deficiency can have serious ramifications for PWSs, including enforcement actions, revocation or suspension of operating permits, fines, and reputational harms. *See* AWWA Decl. ¶¶11-13, 42-43, 45; NRWA Decl. ¶¶16, 39-40; Lane Decl. ¶¶14, 33-35; Pepper Decl. ¶¶12, 22; Walters Decl. ¶¶14, 36-38; *see also* 40 C.F.R. § 141.153(h)(6); *id.* § 142.16(b)(1)-(3), (o)(1)-(2). Reputation and consumer confidence are critical to PWSs, which rely on public trust in their drinking water. *See, e.g., Med. Shoppe Int’l, Inc. v. S.B.S. Pill Dr., Inc.*, 336 F.3d 801, 805 (8th Cir. 2003) (“Loss of intangible assets such as reputation and goodwill can constitute irreparable injury.” (internal quotation marks omitted)). And findings of significant deficiencies may negatively impact a PWS’s credit rating and ability to raise capital. *See* Fitch Wire, *supra* n.5.

The above-described harms to Associations’ members will persist absent a stay pending review.

B. The balance of equities and public interest strongly favor a stay.

The balance of equities and public interest weigh in favor of a stay when “justice requires the court to intervene to preserve the status quo until the merits are determined,” *Glenwood Bridge, Inc. v. City of Minneapolis*, 940 F.2d 367, 370 (8th

Cir. 1991) (internal quotation marks omitted), and when “a stay would preserve the continuity and stability of the regulatory system” pending a review of the merits, *Iowa Utils. Bd.*, 109 F.3d at 426-27. *See Nken*, 556 U.S. at 436 (third factor merges with the public-interest factor when the federal government opposes the relief).

Staying the Cybersecurity Rule will not harm EPA, which has no valid interest in enforcing an unlawful agency action. *See League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016); *Wages & White Lion Invs. v. U.S. FDA*, 16 F.4th 1130, 1143 (5th Cir. 2021). There is “substantial public interest,” however, “in having governmental agencies abide by the federal laws that govern their existence and operations.” *League of Women Voters*, 838 F.3d at 12 (internal quotation marks omitted). *See California v. Azar II*, 911 F.3d 558, 581-82 (9th Cir. 2018) (“The public interest is served from proper [APA] process itself.”).

The public interest favors a stay because there is substantial risk that PWSs and their customers will suffer harms such as decreased credit ratings, increased operating costs, and higher rates for drinking water associated with new compliance costs. *See Teamquest Corp. v. Unisys Corp.*, No. 97cv3049, 2000 WL 34031793, at *19 (N.D. Iowa Apr. 20, 2000) (“The public interest factor frequently invites the court to indulge in broad observations about conduct that is generally recognizable as costly or injurious”); *Fitch Wire*, *supra* n.5; *Walters Decl.* ¶¶28, 35; *Offutt Decl.* ¶¶19, 24. These risks necessarily impact public health because PWSs must take time

and attention away from complying with other SDWA regulations that set standards for lead, copper, arsenic, total coliforms, mercury, benzene, and many other drinking water contaminants. *See* Walters Decl., ¶¶22, 31; Offutt Decl., ¶¶27-28. If this Court stays the Rule, PWSs and their customers will not face these new risks. *See* Walters Decl., ¶42; Offutt Decl., ¶30. The public interest thus weighs strongly in favor of preserving the status quo and allowing PWSs to operate their businesses to continue to provide their customers with clean and safe drinking water. *See New York v. Dep't of Homeland Sec.*, 969 F.3d 42, 87 (2d Cir. 2020) (finding that the public interest favored a preliminary injunction against an agency action that would “likely result in worse health outcomes”) (internal quotation marks omitted); *Whitman-Walker Clinic, Inc. v. Dep't of Health & Human Servs.*, 485 F. Supp. 3d 1, 60-61 (D.D.C. 2020) (finding that, as a result of government action, health providers would “divert already scarce resources” in response to the action, which would also “impede the public interest by threatening the health” of individuals). And while generally well-intentioned, the Rule also *increases* PWSs’ vulnerability to attack by making sensitive cybersecurity information less secure.

III. The Stay Should Apply to All Associations’ Members.

Associations represent thousands of PWSs affected by the Cybersecurity Rule located in all states, territories, and tribal areas. *See* AWWA Decl. ¶¶4, 14; NRWA

Decl. ¶¶3, 14. Associations respectfully request that any preliminary relief crafted by this Court apply to all Associations' members.

“Crafting a preliminary injunction is an exercise of discretion and judgment, often dependent as much on the equities of a given case as the substance of the legal issues it presents.” *Trump v. Int’l Refugee Assistance Project*, 583 U.S. 571, 580 (2017) (per curiam). “[T]he scope of injunctive relief is dictated by the extent of the violation established, not by the geographical extent of the plaintiff class.” *Rodgers v. Bryant*, 942 F.3d 451, 458 (8th Cir. 2019) (quoting *Califano v. Yamasaki*, 442 U.S. 682, 702 (1979)).

The Cybersecurity Rule applies nationwide, and Petitioners and Associations are seeking complete vacatur of the Rule. *See* 5 U.S.C. § 706(2); *Nat’l Min. Ass’n v. U.S. Army Corps of Eng’rs*, 145 F.3d 1399, 1409 (D.C. Cir. 1998) (“[W]hen a reviewing court determines that agency regulations are unlawful, the ordinary result is that the rules are vacated—not that their application to the individual petitioners is proscribed.”). The scope of preliminary relief should therefore reflect the scope of EPA’s violations and the ultimate relief being requested, not simply the number of states that signed onto the petition. *See Rodgers*, 942 F.3d at 458. A stay limited to only the State Petitioners’ jurisdictions would be impractical and would fail “to provide complete relief to” Associations’ members, the majority of which operate outside of Missouri, Arkansas, and Iowa. *Madsen v. Women’s Health Ctr., Inc.*, 512

U.S. 753, 765 (1994); *see, e.g.*, Lane Decl. ¶4 (Colorado); Walters Decl. ¶5 (North Carolina); Pepper Decl. ¶3 (Wyoming).

CONCLUSION

The Court should grant Petitioners-Intervenors' motion to stay the Cybersecurity Rule pending judicial review of the petition for review.

Dated: June 12, 2023

Respectfully submitted,

/s/ Corinne V. Snow

Corinne V. Snow
Vinson & Elkins LLP
1114 Avenue of the Americas
32nd Floor
New York, NY 10036
Phone: (212) 237-0157
Email: csnow@velaw.com

*Counsel for Intervenors American
Water Works Association and
National Rural Water Association*

CERTIFICATE OF COMPLIANCE

This motion complies with the word limit of Fed. R. App. P. 27(d)(2) because it contains 5,150 words, excluding the parts exempted by Fed. R. App. P. 32(f) and 27(d)(2).

This motion complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6), because it has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in Times New Roman 14-point font.

Pursuant to Circuit Rule 28A(h), this motion and its certifications have been scanned for viruses and are virus-free.

Date: June 12, 2023

Respectfully submitted,

/s/ Corinne V. Snow

Corinne V. Snow
Vinson & Elkins LLP
1114 Avenue of the Americas
32nd Floor
New York, NY 10036
Phone: (212) 237-0157
Email: csnow@velaw.com

*Counsel for Intervenors American
Water Works Association and National
Rural Water Association*

CERTIFICATE OF SERVICE

Pursuant to Rule 25 of the Federal Rules of Appellate Procedure, I hereby certify that on June 12, 2023, I electronically filed the foregoing *Petitioners-Intervenors American Water Works Association's and National Rural Water Association's Motion for Stay Pending Review* with the Clerk of the Court for the U.S. Court of Appeals for the Eighth Circuit by using the appellate CM/ECF system, and served copies of the foregoing via the Court's CM/ECF system on all ECF-registered counsel.

Date: June 12, 2023

Respectfully submitted,

/s/ Corinne V. Snow

Corinne V. Snow
Vinson & Elkins LLP
1114 Avenue of the Americas
32nd Floor
New York, NY 10036
Phone: (212) 237-0157
Email: csnow@velaw.com

*Counsel for Intervenors American
Water Works Association and National
Rural Water Association*

Exhibit A

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF G. TRACY MEHAN, III

I, G. Tracy Mehan, III, swear or affirm under penalty of perjury, the following:

1. I am Executive Director of Government Affairs for the American Water Works Association (“AWWA”) and have served in this role since August 1, 2015. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21, and am competent to make this Declaration.

2. Among other things, my responsibilities include helping to advance AWWA’s organizational goals. Through my work as Executive Director of Government Affairs for AWWA, I have become familiar with how the government

regulations for public water systems affect AWWA's members' business operations, which include cybersecurity risk management.

3. AWWA is an international, nonprofit, and scientific and educational society dedicated to providing solutions to ensure the effective management of water. Founded in 1881, AWWA is a 501(c)(3) organization that routinely supports the development of sound water policy for effective public health protection. AWWA is the largest water association in the United States. Our membership includes 4,264 public water systems that supply roughly 80 percent of the nation's drinking water and treat nearly half of the nation's wastewater. AWWA's 50,000-plus members represent the full spectrum of the water community: public and private drinking water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource. AWWA unites a diverse water community to advance public health, safety, the economy, and the environment.

4. Our membership includes 4,264 public water systems, each of which must comply with the Safe Drinking Water Act ("SDWA") and United States Environmental Protection Agency ("EPA" or the "Agency")'s implementing regulations. AWWA's membership includes public water systems in all 50 states and territories.

5. AWWA was formed to promote public health, safety, and welfare through the improvement of the quality and quantity of water. AWWA routinely advocates for water policies at both the legislative and regulatory levels. For example, AWWA was directly engaged in supporting the widely acclaimed 1996 amendments to the SDWA, which require EPA to use a risk and cost assessment and best available peer-reviewed science when developing regulatory standards in order to focus attention on the most important health threats.

6. AWWA also routinely files public comments on rulemakings that will impact its members through the public notice and comment periods provided under the Administrative Procedure Act (“APA”). AWWA views this as a necessary and important part of its role in representing its membership and carrying out its mission.

7. AWWA’s government affairs mission is to: (1) advocate for effective laws, regulations, programs and policies that ensure safe and affordable water for all Americans; (2) support effective measures that protect America’s irreplaceable sources of drinking water; and (3) help water utilities function as high-performing and sustainable business enterprises (whether municipal or investor owned) so they can provide excellent service to their customers, today and over the long run.

8. I am familiar with EPA’s March 3, 2023, memorandum entitled “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process” (“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises

EPA’s interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems to require evaluation of a system’s cybersecurity measures. I am also familiar with accompanying guidance document, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance”), available at <https://tinyurl.com/bdfhfrdj>. Despite creating new regulatory obligations for states and public water systems, neither the Cybersecurity Rule nor Guidance were subject to notice and comment pursuant to the APA prior to issuance.¹ As a result, AWWA was not afforded an opportunity to comment on either document through the APA procedures.

9. I am familiar with EPA’s regulations for states with primacy under the SDWA. Having a sanitary survey program is one of several preconditions necessary for a state to be delegated primacy under SDWA. EPA’s regulations require states to conduct periodic sanitary surveys at public water systems to evaluate eight elements as applicable to the system: (1) source, (2) treatment, (3) distribution system, (4) finished water storage, (5) pumps, pump facilities, and controls, (6) monitoring, reporting, and data verification, (7) system management and operation,

¹ EPA invited public comment on certain aspects of the Cybersecurity Guidance, noting that it would “revise and update” the Guidance “as needed based on public comment and new information.” EPA, Evaluating Cybersecurity During Public Water System Sanitary Surveys 2 (2023). However, EPA is accepting comments only through a specific agency email address rather than a publicly available docket otherwise published on the *Federal Register* for notice-and-comment rulemakings.

and (8) operator compliance with state certifications. *See* 40 C.F.R. §§ 141.2, 142.16(b)(3), 142.16(o)(2).

10. EPA’s regulations for states with primacy include the provisions that states “must conduct sanitary surveys for all surface water systems (including groundwater under the influence) that address the eight sanitary survey components listed in [40 C.F.R. § 142.16(b)(3)(i)(A)-(H)] no less frequently than every three years for community systems and no less frequently than every five years for noncommunity systems.” *Id.* § 142.16(b)(3)(i). AWWA’s members include both community water systems and noncommunity water systems that are subject to periodic sanitary surveys. AWWA’s members include public water systems that are due for or have been notified that they will be subject to a sanitary survey in the next six months.

11. As part of the sanitary survey, a state with primacy is required to identify any “significant deficiencies”—meaning defects, failures, malfunctions, or similar deficiencies that are causing or have the potential to cause the introduction of contamination into drinking water delivered to customers—and use its authority to require a public water system to address any identified significant deficiencies. *See id.* §§ 142.16(b)(1)–(3), (o)(1)–(2).

12. From experience, I know that the risk of a significant deficiency is a serious concern for any our public water system members and these members

therefore take proactive steps in advance of a sanitary survey to avoid such findings. Members have expressed concerns related to significant deficiencies that include the potential for misinformation in the media, reputational harm, and fines that can result.

13. It is my understanding that the Cybersecurity Rule mandates that states, in the course of conducting a sanitary survey, must now evaluate public water systems' cybersecurity controls and identify potential cybersecurity-related "significant deficiencies," which systems would then need to correct. It is also my understanding that the Cybersecurity Guidance identifies a checklist of specific cybersecurity controls of varying complexity and cost, found at Appendix A, that EPA recommends states should use for evaluating cybersecurity during sanitary surveys, and that the absence (or inadequacy) of one or more of those controls could be deemed a "significant deficiency" that would require correction by the public water system.

14. AWWA's membership includes 4,264 public water systems, including Benton Washington Regional Public Water Authority ("Benton"), Platte Canyon Water and Sanitation District ("Platte Canyon"), City of Ames Water & Pollution Control Department ("City of Ames"), Davidson Water Company ("Davidson Water"), and City of and Borough of Sitka, Alaska ("City of Sitka"), all of which are subject to the Cybersecurity Rule.

15. EPA, rather than the state, directly oversees the sanitary survey program in Wyoming, the District of Columbia, as well as for Tribes. AWWA's membership includes public water systems in both Wyoming and the District of Columbia.

16. AWWA's membership includes public water systems serving over 3,300 people who are subject to the cybersecurity requirements in America's Water Infrastructure Act of 2018 ("AWIA"). AWWA's membership also includes public water systems serving fewer than 3,300 people who are not subject to the cybersecurity requirements in AWIA.

17. AWWA's membership includes water systems that are subject to the Cybersecurity Rule because they use an industrial control system or other operational technology as part of the equipment or operation of a required component of the sanitary survey.

18. As part of its mission, AWWA has been actively involved in assisting public water systems in evaluating, addressing, and managing cybersecurity risks, and has issued reports and risk management tools for its members. *See, e.g.,* Judith H. Germano, AWWA, *Cybersecurity Risk & Responsibility in the Water Sector* (2019), <https://tinyurl.com/2p8m8y5x>; *Cybersecurity Risk Management Tool*, AWWA, <https://tinyurl.com/bdeubdac> (last visited Apr. 26, 2023). AWWA has also hosted informational and technical conferences on the subject. AWWA also

frequently engages with Members of Congress to discuss and advocate for the best approaches to cybersecurity resilience and oversight.

19. AWWA believes that cybersecurity is mission-critical for all types of water utilities. As such, we support efforts to strengthen cybersecurity and are eager to collaborate with EPA to develop and implement effective approaches for public water systems. However, EPA's decision to add cybersecurity requirements to the sanitary survey program for drinking water utilities is ill-advised, impractical, and not designed to meaningfully improve system resiliency.

20. With respect to the Cybersecurity Rule in particular, AWWA has frequently advocated against EPA's approach of using sanitary surveys as the vehicle for conducting cybersecurity evaluations in letters and comments to the Agency. For example, shortly before EPA's issuance of the Cybersecurity Rule, AWWA, along with other interested associations, submitted a letter to EPA.

21. In this letter AWWA objected to, among other things, the Agency's treatment of the Cybersecurity Rule as an interpretative, rather than legislative, rule; the lack of adequate stakeholder engagement with representatives of state and local governments and interested associations, like the AWWA; and EPA's insistence on using sanitary survey programs as the vehicle for conducting cybersecurity evaluations. *See* Letter to Michael Regan, Administrator, U.S. Env't Prot. Agency, from Am. Water Works Ass'n et al. (Jan. 25, 2023), <https://tinyurl.com/29us4ap7>.

22. The letter also raised the concern that state sanitary survey programs are likely to lack the appropriate staffing, training, and expertise to properly and effectively evaluate cybersecurity programs, increasing the likelihood of unmerited findings of deficiency. *Id.* at 7–8. At AWWA, we continue to have these concerns with EPA’s proposed approach as a result of conversations I and others have had with state staff members in multiple states. After EPA’s issuance of the Cybersecurity Rule, AWWA reiterated its concerns in a letter to the Agency, noting that EPA had failed to substantively analyze the burdens on states and public water systems associated with using sanitary survey programs to conduct cybersecurity evaluations, as well as underestimated the burden on public water systems to implement the necessary cybersecurity controls and prepare for state evaluations during sanitary surveys. *See* Letter to Michael Regan, Administrator, U.S. Env’t Prot. Agency, and Richard Revesz, Administrator, Office of Info. & Regul. Affs., from Am. Water Works Ass’n et al. (Apr. 24, 2023), <https://tinyurl.com/2a3dawc3>.

23. AWWA members subject to the Cybersecurity Rule have raised these and other concerns with the requirements in discussions with AWWA staff, including myself. These concerns include data handling to protect data related to their sensitive cybersecurity practices from public disclosure. From discussions with members, I know that some members feel that they must address all thirty-six

“recommendations” in EPA’s Guidance in order to avoid a significant deficiency in their next sanitary survey.

24. Because EPA did not provide an APA notice and comment period for the Cybersecurity Rule prior to finalizing the rule, AWWA was unable to use the public comment period as an avenue to formally express its views and concerns and ensure that the Agency take them into consideration before finalizing this rule. Because EPA did not provide a public notice and comment period for the Cybersecurity Rule, it is unknown the extent to which EPA considered comments provided by AWWA prior to the release of the rule.

25. Ultimately, we fear the sanitary survey approach adopted by EPA could do more harm than good for drinking water utilities and the public.

26. Presently, states take differing approaches to addressing cybersecurity for public water systems. Some of our public water system members are located in states that already have state law requirements for cybersecurity that apply to our members. These members will incur costs and burdens associated with determining whether and how they must adjust their current cybersecurity practices to meet the new Cybersecurity Rule requirements.

27. Other members are located in states that do not presently have state law cybersecurity requirements that apply to our members. These members will incur

costs based on the new requirements states will be forced to impose as a result of the Cybersecurity Rule.

28. As part of my role at AWWA, I am familiar with the financial, budgetary, operational, and staffing difficulties that new requirements like the Cybersecurity Rule place on our public water system members. These members include public and quasi-public systems with limited budgets and other constraints on their ability to quickly implement budgetary changes. Some of our members must receive approval from elected bodies in order to make such changes. In most cases, additional costs will ultimately be passed on to rate-paying customers in the form of higher costs for the drinking water they receive. Such costs can be particularly difficult for small systems that serve a limited number of customers.

29. Due to the public or quasi-public nature of many public water system members, they often need time in advance of new requirements to submit budget proposals to the bodies that approve their budgets. Even for our private water system members, it can be difficult to quickly adjust rates to respond to new regulatory requirements.

30. As a result of these considerations, AWWA regularly provides comments on the costs and burdens associated with EPA's proposals for new regulatory requirements that would impact AWWA's members. AWWA also

regularly provides recommendations to the Agency regarding how it can limit burdens on public water systems.

31. AWWA has consulted and engaged with its public water system members to discuss the likely costs and burdens associated with the Cybersecurity Rule and Guidance. Administrative costs to public water systems associated with changes in regulations, like those contained in the Cybersecurity Rule, include the initial costs and internal labor hours to understand a new rule and provide training to staff regarding a new rule's requirements. This is especially true when considering the kinds of documentation and verification requirements associated with sanitary surveys when combined with the complexity of cybersecurity—an area of operations that many of our members have not previously had to explicitly document in the manner prescribed by the Cybersecurity Rule and Guidance.

32. Our public water system members will also have to familiarize themselves with the specific requirements in the Cybersecurity Rule. These costs include a six-hour training course for public water systems provided by EPA for familiarization.

33. Additionally, the Cybersecurity Rule and Guidance rely upon a thirty-six item checklist of cybersecurity controls that states should look for and evaluate when conducting sanitary surveys, including thirty-three that are likely to apply to Public Water Systems. Some of these controls are complex and/or costly measures,

such as maintaining and updating inventories, configurations, and network topologies of operational technology (“OT”) and information technology (“IT”) assets, and evaluating the cybersecurity measures of third-party vendors and contractors during procurement processes. Additionally, EPA specifically identifies sixteen of these controls as “potential significant deficiencies.”

34. EPA states that these controls are “Technically feasible for most PWSs to address without significant capital expenditures”. EPA has not provided any information to support that statement nor has it provided a burden assessment as required by the Paperwork Reduction Act which would offer some insight on expected impact of the rule on different size utilities with varying capacity. Review of the controls in the context of a compliance regiment by subject matter experts indicates that many of these controls would require capital investments to support conformity.

35. For example, Control 3.1 calls on the utility to “Collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation.” This control appears to require a baseline intrusion detection system (“IDS”). AWWA has been informed that typically, an IDS is implemented as part of a demilitarized zone boundary (“DMZ”) separating the IT and OT networks. Costs for these systems vary by device count but a minimum capital expense for base level systems may start at approximately \$10,000.

Supporting subscriptions are also variable but can start around \$250 per node. This often also includes technology for a security information and event management (“SIEM”) to manage the monitoring and alerting functions, such as password attempts and log monitoring. AWWA has been informed that average price of SIEM is approximately \$50,000 and may range from minimum of \$20,000 to upwards of \$1 million depending on the complexity of the entity’s operations.

36. These are not onetime capital investments and require ongoing maintenance to support them, including the personnel that must be employed directly or indirectly via third-party support services to maintain the integrity of these systems. While many entities likely have some level of investment for these systems, consideration must be given to range of entities that may require additional investment to support this requirement.

37. While AWWA has repeatedly engaged with the Agency on cybersecurity related issues, AWWA was not aware of the specific requirements, including the checklist of thirty-six cybersecurity controls, until EPA issued the Cybersecurity Rule.

38. Due to the complexity of the controls, combined with the typical budgetary constraints facing many public water systems, some of our public water system members may not currently have all thirty-six controls in place. Some of our public water system members have therefore indicated to us that they will incur

significant monetary and internal and/or external labor costs in order to assessment existing cybersecurity controls, evaluate conformance to the thirty-six item checklist, and plan implementation of any controls not currently in place—all of which must be completed prior to a system’s next sanitary survey.

39. To further compound problems, over 93 percent of public water systems serve fewer than 3,300 persons and have limited capacity to support staff dedicated to managing cybersecurity. In addition, many public water systems are part of a local municipal government in which technology-based systems are centrally managed and supported. These member systems therefore feel compelled to either hire full-time cybersecurity professionals with specialized (*i.e.*, costly) knowledge and experience of the cybersecurity needs of public water systems, or hire third-party contractors and consultants with similar expertise. These are additional costs public water systems would likely bear due to the Cybersecurity Rule that do not seem to have been accounted for by the Agency. Because no economic impact assessment was released with the Cybersecurity Rule, AWWA has not been able to review or comment on any cost assessment associated with the rule.

40. Some of AWWA’s public or quasi-public members share IT or cybersecurity services with broader local government entities and do not have control over staffing, operational, and budget decisions for these functions.

41. AWWA's members include public water systems that have reported to AWWA that they have been informed by regulators that they must conduct a third party assessment of their cybersecurity practices as a result of the Cybersecurity Rule. These members have reported that they will incur costs, including in the form of internal or external labor, in order to comply with this new requirement.

42. The Cybersecurity Rule states that “[f]or groundwater systems, states must maintain records of written notices of significant deficiencies and confirmation that a significant deficiency has been corrected.” As part of my work on these issues, I have learned that public disclosure laws vary from state to state. Not all state laws in states where our members are located protect information collected through sanitary surveys by state agencies from being shared with the public. As a result, members have shared concerns about the increased risks they face from this information being disclosed now that states are required to collect such information. Some states where our members operate lack the explicit authority to isolate this class of information from the rest of the compliance data collected by the state as part of the sanitary survey.

43. In addition, EPA regulations require states to provide compliance data to EPA, including reports of sanitary surveys, and a record of the most recent vulnerability determination. *See* 40 C.F.R. § 142.14. As a result, we are concerned that sensitive cybersecurity information from our members would become subject to

disclosure under the Freedom of Information Act as a result of the Cybersecurity Rule. The rule therefore increases risks to our members.

44. Even if information about cybersecurity-related deficiencies are made confidential, there is still the acute risk of the state maintaining a centralized database of information concerning the potential cybersecurity vulnerabilities of all public water systems in its jurisdiction—a repository that itself might be vulnerable to a cyberattack.

45. Additionally, because “significant deficiencies” recorded during a public water system’s sanitary survey must be included in the system’s annual “consumer confidence report”—which a system must make publicly available to its customers—AWWA’s members have voiced concerns about the risks of making public any potential cybersecurity vulnerabilities. Making such information public in a centralized database or similar repository may turn particular systems into targets for hackers or other bad actors seeking to leverage potential vulnerabilities for their own nefarious purposes.

46. Given the sensitive nature of cybersecurity our members are very concerned that the rule may result in public disclosure of a “significant deficiency” which may be leveraged by malicious actors to attack a system. The Cybersecurity Rule creates a new recordkeeping obligation on states for tracking compliance with the sanitary survey program which is a matter of public record that cannot reasonable

be segmented from related compliance information. This places the utility operations and the public at increased risk that is not in the interest of national security.

47. AWWA's members, such as Benton, City of Ames, Platte Canyon, Davidson Water, and City of Sitka, will not incur the above-described costs and burdens associated with the Cybersecurity Rule if the rule is found unlawful and set aside.

48. I have spoken to multiple AWWA members located in multiple different states since EPA issued the Cybersecurity Rule who have indicated that they are already incurring costs and making operational changes in response to the Cybersecurity Rule. Some of these members have indicated that they are taking these steps in advance of their next sanitary survey to avoid a potential finding of a significant deficiency. Some of these members have also indicated that they do not believe they can wait to begin to incur these costs because EPA indicated that the Cybersecurity Rule is immediately effective.

49. I have spoken to multiple AWWA members located in multiple different states who have indicated that their state regulators have not previously inquired about their cybersecurity practices during past sanitary surveys. I am not aware of any past EPA guidance for sanitary surveys that define cybersecurity measures that may be evaluated as part of a sanitary survey. I am not aware of any

member previously receiving a significant deficiency as a result of their cybersecurity practices during a sanitary survey.

50. Given the sensitive nature of cybersecurity and the potential increased risks that could result if members publicly disclose their current practices, many of our members are unwilling to publicly state which of the items on EPA’s list of specific “potential significant deficiencies” they do not currently have in place or to otherwise disclose information about their current cybersecurity practices. This makes AWWA’s advocacy on these issues all the more important for its members, as AWWA is able to raise concerns without directly attributing the concerns to an individual member or system.

51. I am familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa (“Petitioners”), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule. Because the Cybersecurity Rule is likely to increase the regulatory burden and associated costs on some of AWWA’s members, increase cybersecurity risks for some members and the public, and result in a regulatory scheme that is not beneficial for America’s water users, this lawsuit is germane to AWWA’s purpose to advocate for effective laws, regulations, programs and policies that ensure safe and affordable water for all Americans and help water utilities function as high-performing and sustainable business enterprises.

52. This case is also germane to AWWA’s purpose because the Petitioners’ requested relief—holding the Cybersecurity Rule unlawful and setting it aside—would alleviate the administrative and operational costs and burdens the rule places on AWWA’s members, such as Benton, City of Ames, Platte Canyon, Davidson Water, and City of Sitka, and more than 4,000 other public water systems. It would also alleviate the increased risk of cybersecurity attacks due to public records disclosing a “significant deficiency” that this rule creates for some members.

53. Because EPA has improperly treated the Cybersecurity Rule as an interpretive rule, AWWA, like other interested parties, has thus far not been afforded a formal opportunity to raise its comments regarding and concerns about the Cybersecurity Rule, such as those described herein, pursuant to APA notice and comment. As such, AWWA has not been afforded opportunity to protect its members’ interests in avoiding excessive, ineffective, potentially harmful, or unlawful regulatory obligations through a fair and transparent regulatory process.

54. If EPA is required to instead promulgate cybersecurity requirements for public water systems through the APA’s notice and comment rulemaking process, then AWWA will have the opportunity to participate in the rulemaking process and provide specific feedback on EPA’s proposed requirements and proposed implementation timeline. AWWA intends to participate in any such future rulemaking process.

55. Our members have many years of experience with both sanitary surveys and cybersecurity, and they believe that using sanitary surveys will be ineffective at improving cybersecurity at water systems and will result in significant implementation challenges for both our members and the states. As part of our mission, AWWA is committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. AWWA would like the opportunity to propose more workable solutions to EPA than the approach taken by EPA in the Cybersecurity Rule.

56. AWWA recognizes 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, using an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector than the one imposed by EPA through the Cybersecurity Rule.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 16 day of May, 2023.

A handwritten signature in black ink that reads "G. Tracy Mehan, III". The signature is written in a cursive style with a vertical line to the right of the text.

G. Tracy Mehan, III
Executive Director Government Affairs
American Water Works Association

Exhibit B

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF MATTHEW HOLMES

I, Matthew Holmes, swear or affirm under penalty of perjury, the following:

1. I am Chief Executive Officer for the National Rural Water Association (“NRWA”) and have served in this role since July 1, 2020. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21, and am competent to make this Declaration.

2. Among other things, my responsibilities include administration of day-to-day operation, maintaining an effective government affairs program, overseeing advocacy on regulations affecting the membership, building relationships within the water sector, and serving as spokesman for the association.

3. NRWA, founded in 1976, is a nonprofit organization dedicated to training, supporting, and promoting water and wastewater professionals that serve small communities across the United States. NRWA is the country's largest water utility association, representing over 15,000 public water system members through its 50 affiliated State Rural Water Associations in all 50 states. NRWA's programs generally focus on assisting small and rural communities serving fewer than 10,000 people and cover all aspects of operating, managing, and financing water and wastewater utilities. Most notably, through our "Circuit Rider" program, drinking water professionals from our affiliate network provide in-person, hands-on assistance and training for small, rural systems on an everyday basis. In 2022, NRWA and state affiliate staff provided on-site technical assistance visits and spent more than 200,000 hours training more than 65,000 utilities.

4. As public water systems, our members are required to comply with the Safe Drinking Water Act ("SDWA") and United States Environmental Protection Agency ("EPA" or the "Agency") implementing regulations.

5. NRWA frequently advocates for water policies at both the legislative and regulatory levels that ensure small and rural utilities have the support and resources necessary to serve their communities, urging legislators and regulators to consider approaches to regulation that ensure access to safe and affordable water for all Americans while also accounting for the unique operations and character of the

myriad public water systems across the United States. From experience, NRWA believes that enhancing drinking water quality is more often a resource problem rather than a regulatory one.

6. To that end, NRWA routinely files public comments on SDWA rulemakings that will impact its members, availing itself of the public notice-and-comment periods provided under the Administrative Procedure Act (“APA”). We have done so for a variety of EPA proposed regulations under the SDWA, such as the Agency’s revisions to its lead and copper standards and its perchlorate standards. *See* Nat’l Rural Water Ass’n, Comments on Proposed Rule, National Primary Drinking Water Regulations: Proposed Lead and Copper Rule Revisions, 84 Fed. Reg. 61,684 (Feb. 11, 2020) (“LCR Comments”), *available at* <https://tinyurl.com/bdcnkybs>; Nat’l Rural Water Ass’n, Comments on Proposed Rule, National Primary Drinking Water Regulations: Perchlorate, 84 Fed. Reg. 30,524 (Aug. 26, 2019), *available at* <https://tinyurl.com/29buztff>. NRWA believes its participation in the regulatory process is a necessary and important part of its role as representative of its members and is essential in carrying out its mission to protect the interests of small and rural water systems.

7. NRWA has permanent standing Regulatory and Legislative Committees that consist of Board Members that actively manage or operate rural

water systems nationwide. Since inception, NRWA has also maintained a permanent legislative and regulatory staff in Washington, D.C.

8. Each year NRWA conducts a Rural Water Conference in Washington, D.C. attended by hundreds of rural utility industry representatives from all 50 states and Puerto Rico. This venue is used to interact with policy leaders within the EPA and other federal agencies to address current or proposed policy issues affecting the rural water industry. Attendees meet with their Congressional delegations to directly advocate for appropriation priorities that include, but are not limited to, the Safe Drinking Water State Revolving Loan Fund and the Clean Water State Revolving Loan Fund.

9. NRWA also provides recommendations to Congress on legislation and policy related issues regarding the Safe Drinking Water Act and the potential impacts on small and rural utilities.

10. Many of NRWA's members are very small utilities that rely on NRWA to ensure regulations are fair, achievable, and written to avoid financial hardships. Many of our utility members have only one to two employees and will require technical assistance, financial assistance, and time to implement sweeping cybersecurity requirements.

11. I am familiar with EPA's March 3, 2023, memorandum entitled "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process"

(“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises EPA’s interpretations of its SDWA regulations regarding state-conducted periodic sanitary surveys of public water systems. The revisions require states to evaluate public water systems’ cybersecurity systems as part of sanitary surveys. I am also familiar with the accompanying guidance document, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance”), available at <https://tinyurl.com/bdfhfrdj>.

12. Despite creating new regulatory obligations for states and public water systems, it is my understanding that neither the Cybersecurity Rule nor Guidance were subject to notice and comment pursuant to the APA prior to issuance. As a result, NRWA was not afforded an opportunity to formally comment on either document. As active participants in this process, NRWA would have provided comments had cybersecurity requirements been introduced as a proposed rule with opportunity for comment under the APA.

13. I am generally familiar with EPA’s regulations for states with primacy under the SDWA. As a precondition for state primacy under the SDWA (*i.e.*, allowing states to directly administer the SDWA within its borders), EPA’s regulations require a state to establish a program for conducting “sanitary surveys for all surface water systems (including groundwater under the influence) that address the eight sanitary survey components listed in [40 C.F.R.

142.16(b)(3)(i)(A)–(H)] no less frequently than every three years for community systems and no less frequently than every five years for noncommunity systems.” 40 C.F.R. § 142.16(b)(3)(i). A sanitary survey is essentially an on-site review of a system’s water source, facilities, equipment, and operations and maintenance in order to evaluate its adequacy to produce and distribute safe drinking water. *See id.* §§ 141.2, 142.16(b)(3), 142.16(o)(2).

14. NRWA’s members include both community water systems and noncommunity water systems that are subject to periodic sanitary surveys, including Davidson Water, Inc. (“Davidson Water”). Public Water Supply District #2, Andrew County, Missouri (“District #2”), City of Clinton Water and Sewer Department (“Clinton”), Public Water Supply District #4, Platte County, Missouri (“District #4”), and Mahaska Rural Water System, Inc. (“Mahaska”). Wyoming Association of Rural Water Systems (“WARWS”) is a state affiliate member of NRWA with public water system members that are subject to periodic sanitary surveys.

15. As part of a survey, a state is required to identify any “significant deficiencies”—meaning defects, failures, malfunctions, or similar deficiencies that are causing or have the potential to cause the introduction of contamination into drinking water delivered to customers—and use its authority to require a public water system to address any identified significant deficiencies. *See id.* § 142.16(b)(1)–(3), (o)(1)–(2).

16. From experience, I know that the risk of a finding of significant deficiency poses concerns for many of our public water system members. Our members therefore often take proactive steps in advance of a sanitary survey to avoid such findings. Members frequently express concern that a finding of significant deficiency, which are generally made public to customers, risks undermining customer confidence, on top of the possibility of monetary fines or other corrective action from regulators.

17. It is my understanding that the Cybersecurity Rule and Guidance require states in the course of conducting sanitary surveys to now evaluate public water systems' cybersecurity controls and identify potential cybersecurity-related "significant deficiencies," which systems would then need to correct. It is also my understanding that the Cybersecurity Guidance identifies a checklist of specific cybersecurity controls of varying complexity and cost, found at Appendix A, that states should look for and evaluate during sanitary surveys, and that the absence (or inadequacy) of one or more of those controls could be deemed a "significant deficiency" that would require correction by the public water system.

18. NRWA's membership, through its state affiliates, includes over 15,000 public water systems, including Davidson Water, District #2, Clinton, District #4, and Mahaska, all of which are subject to the Cybersecurity Rule.

19. EPA, rather than the state, directly oversees the sanitary survey program in Wyoming and the District of Columbia. NRWA's membership includes public water systems in Wyoming.

20. NRWA's membership includes public water systems serving over 3,300 people who are subject to the cybersecurity requirements in America's Water Infrastructure Act of 2018 ("AWIA"). NRWA's membership also includes public water systems serving fewer than 3,300 people who are not subject to the cybersecurity requirements in AWIA.

21. As part of its mission, NRWA has been actively involved in assisting public water systems in evaluating, addressing, and managing cybersecurity risks. For example, NRWA has partnered with the Mission Critical Global Alliance ("MCGA") to establish a comprehensive and continuous cyber education program that helps small and rural water systems manage their particular cybersecurity risks and safeguard their operational technology ("OT") and information technology ("IT") assets. This program provides NRWA members with critical cybersecurity training, through organized courses and certification trainings, as well as on-site, hands-on training through our "Circuit Rider" program, where drinking water professionals provide assistance to member systems on an everyday basis. NRWA also frequently engages with elected representatives and regulators to discuss and advocate for the best approaches to cybersecurity resilience and oversight for small

and rural water systems, which often lack the necessary expertise and/or resources to implement robust cybersecurity measures.

22. NRWA believes that cybersecurity is mission-critical for all types of water utilities, especially those in small and rural communities who can be more vulnerable to service disruptions. As such, we support efforts to strengthen cybersecurity, and are eager to collaborate with EPA to develop and implement effective approaches for public water systems. EPA's decision, however, to add cybersecurity requirements to the sanitary survey program for drinking water is unlikely to meaningfully improve system resiliency and may ultimately be counterproductive to that goal.

23. NRWA has advocated against EPA's approach of using sanitary surveys as the vehicle for conducting cybersecurity evaluations in letters and comments to the Agency. For example, shortly before EPA's issuance of the Cybersecurity Rule, NRWA, along with other interested associations like the American Water Works Association ("AWWA"), submitted a letter to EPA voicing its concerns with such an approach. In this letter, NRWA objected to, among other things, the Agency's treatment of the Cybersecurity Rule as an interpretative, rather than legislative, rule; the lack of adequate stakeholder engagement with representatives of state and local governments and interested associations, like NRWA; and EPA's insistence on using sanitary survey programs as the vehicle for

conducting cybersecurity evaluations. *See* Letter to Michael Regan, Administrator, U.S. Env't Prot. Agency, from Nat'l Rural Water Ass'n et al. (Jan. 25, 2023), <https://tinyurl.com/29us4ap7>. The letter also raised the concern that state sanitary survey programs are likely to lack the appropriate staffing, training, and expertise to properly and effectively evaluate cybersecurity programs, increasing the likelihood of unmerited findings of deficiency. *Id.* at 7–8. At NRWA, we continue to have these concerns with EPA's proposed approach as a result of conversations I and others have had with state staff members in multiple states.

24. In discussions with NRWA staff, including myself, NRWA members subject to the Cybersecurity Rule have raised these and other concerns with the Rule's requirements.

25. Because the Cybersecurity Rule was not subject to APA notice and comment, NRWA was unable to use the public comment period as an avenue for NRWA to formally express its views and concerns and ensure that the Agency take them into consideration before finalizing its Rule. As EPA did not provide a public notice-and-comment period for the Cybersecurity Rule, it is unknown the extent to which EPA considered NRWA's comments.

26. Ultimately, we fear the sanitary survey approach adopted by EPA could do more harm than good for drinking water utilities and the public.

27. Presently, states take differing approaches to addressing cybersecurity for public water systems. Some of our public water system members are located in states that already have state requirements for cybersecurity that apply to our members. These members will incur costs and burdens associated with determining whether and how they must adjust their current cybersecurity practices to meet the new Cybersecurity Rule requirements. Other members are located in states that do not presently have cybersecurity requirements that apply to our members. These members will incur costs based on the new requirements states will be forced to impose as a result of the Cybersecurity Rule.

28. As part of my role at NRWA, I am familiar with the financial, budgetary, operational, and staffing difficulties that new regulatory requirements like those imposed by the Cybersecurity Rule place on small and rural public water systems. Many of these systems include public and quasi-public systems with limited budgets and other constraints on their ability to quickly implement budgetary changes, such as the need for approval by local governing bodies. The imposition of additional, unfunded regulatory requirements will only serve to further strain the budgets of smaller communities. In most cases, additional costs will ultimately be passed on to rate-paying customers in the form of higher costs for the drinking water they receive. Such costs can be particularly difficult for small systems that serve a limited number of customers.

29. As a result of these considerations, NRWA regularly provides comments on the costs and burdens associated with EPA's proposals for new regulatory requirements that would impact NRWA's members. NRWA also regularly provides recommendations to the Agency regarding how it can limit burdens on public water systems. *See, e.g.*, LCR Comments, at 6, 8.

30. NRWA has consulted and engaged with its public water system members to discuss the likely costs and burdens associated with the Cybersecurity Rule and Guidance. Administrative costs to public water systems associated with changes in regulations, like those contained in the Cybersecurity Rule, include the initial costs and internal labor hours to understand a new rule and provide training to staff regarding a new rule's requirements. This is especially true when considering the complexity of cybersecurity, an aspect of water system management that is likely to be less familiar to the typical public water system than, say, pollutant control. For the Cybersecurity Rule, these costs include a six-hour training course for public water systems provided by EPA.

31. Additionally, the Cybersecurity Rule and Guidance rely upon a thirty-six item checklist of cybersecurity controls that states should look for and evaluate when conducting sanitary surveys. Some of these controls are complex and/or costly measures, such as maintaining and updating inventories, configurations, and network topologies of operational technology ("OT") and information technology

(“IT”) assets, and evaluating the cybersecurity measures of third-party vendors and contractors during procurement processes.

32. While NRWA has repeatedly engaged with the Agency on cybersecurity related issues, NRWA was not aware of the specific requirements of the Cybersecurity Rule, including the checklist of thirty-six potential significant deficiencies, until issued by EPA.

33. Due to complexity of the controls, combined with the typical budgetary, staff, and expertise constraints facing many small and rural water systems, some of our members do not currently have all thirty-six controls in place. Some of our members have therefore indicated to us that they will incur significant monetary and internal and/or external labor costs in order to audit existing cybersecurity controls, evaluate conformance to the thirty-six item checklist, and implement those controls not currently in place—all of which must be completed prior to a system’s next sanitary survey.

34. To further compound problems, many of our public water system members lack dedicated cybersecurity professionals on staff. These member systems therefore feel compelled to either hire full-time cybersecurity professionals with specialized (*i.e.*, costly) knowledge and experience of the cybersecurity needs of public water systems, or hire third-party contractors and consultants with similar expertise. These are additional costs public water systems would likely bear due to

the Cybersecurity Rule. Some of our smallest members, in fact, rely on volunteer staff to maintain operations, making it all the more unlikely that they will have the resources to hire or contract with a qualified cybersecurity professional.

35. Further, some of NRWA's public or quasi-public members share IT or cybersecurity services with broader local government entities and do not have control over staffing, operational, and budget decisions for these functions.

36. With respect to outside cybersecurity professionals, some members have expressed concern with using third-party contractors, as these contractors are often selling particular products or services, meaning that their recommendations may not be in our members' best interest in providing safe and affordable drinking water to their communities.

37. NRWA's members include public water systems that have reported to NRWA that they have been informed by their state regulators that they must conduct a self-assessment or third party assessment of their cybersecurity practices as a result of the Cybersecurity Rule. These members have reported that they will incur costs, including in the form of internal or external labor, in order to comply with this new requirement.

38. Regarding the risk of a finding of significant deficiency, NRWA and its members are concerned that the limited cybersecurity expertise and experience of state officials conducting sanitary surveys may lead to the recordation of

erroneous or ill-founded cybersecurity-related significant deficiencies. In other words, state officials with limited training in evaluating cybersecurity resilience may be too quick to record significant deficiencies—a problem compounded by the potential for undue reliance on a rigid checklist—without properly evaluating whether the purported deficiency actually affects water system operations or security.

39. Additionally, because “significant deficiencies” recorded during a public water system’s sanitary survey are included in the system’s annual “consumer confidence report”—which a system must make publicly available to its customers—NRWA’s members have voiced concerns about the risks of making public any potential cybersecurity gaps. Making such information public in a centralized database or similar repository may turn particular systems into targets for hackers or other bad actors seeking to leverage potential vulnerabilities for their own nefarious purposes. This is particularly true for smaller, rural systems that already may be perceived as less sophisticated and therefore more vulnerable to cyberattack given, as compared to larger, urban water systems.

40. The Cybersecurity Rule states that “[f]or groundwater systems, states must maintain records of written notices of significant deficiencies and confirmation that a significant deficiency has been corrected.” Cybersecurity Rule, at 5. As part of my work on these issues, I have learned that public disclosure laws vary from

state to state. Not all state laws in states where our members are located protect information collected through sanitary surveys by state agencies from being shared with the public. As a result, members have shared concerns about the increased risks they face from this information being disclosed now that states are required to collect such information.

41. Even if information about cybersecurity-related deficiencies are made confidential, there is still the acute risk of the state maintaining a centralized database of information concerning the potential cybersecurity vulnerabilities of all public water systems in its jurisdiction—a repository that itself might be vulnerable to a cyberattack.

42. NRWA's members, including Davidson Water, District #2, Clinton, District #4, and Mahaska will not incur the above-described costs and burdens associated with the Cybersecurity Rule if the Rule is found unlawful and set aside.

43. I have spoken to multiple NRWA members located throughout the United States since EPA issued the Cybersecurity Rule, and those members have indicated that they are already incurring costs and making operational changes in response to the Cybersecurity Rule. Some of these members have indicated that they are taking these steps in advance of their next sanitary survey to avoid a potential finding of a significant deficiency. Some of these members have also indicated that

they do not believe they can wait to begin to incur these costs because EPA indicated that the Cybersecurity Rule is immediately effective.

44. I have spoken to multiple NRWA members located in multiple different states who have indicated that their state regulators have not previously inquired into their cybersecurity practices during past sanitary surveys. I am not aware of any past EPA guidance indicating that cybersecurity measures should be evaluated as part of a sanitary survey. I am not aware of any member previously receiving a significant deficiency as a result of their cybersecurity practices.

45. Given the sensitive nature of cybersecurity and the potential increased risk of cyberattack that could result if members are required to discuss their current practices publicly, many of our members are unwilling to publicly state which of the items on EPA's list of specific "potential significant deficiencies" they do not currently have in place or to otherwise disclose information about their current cybersecurity practices. This makes NRWA's advocacy on these issues all the more important for its members, as NRWA is able to raise concerns without directly attributing the concerns to an individual member or system.

46. I am familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa ("Petitioners"), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule. Because the Cybersecurity Rule is likely to increase the costs to some of NRWA's members, increase cybersecurity

risks for some members, and result in regulation that is not beneficial for America's water users, this lawsuit is germane to NRWA's purpose.

47. This case is also germane to NRWA's purpose because the Petitioners' requested relief—holding the Cybersecurity Rule unlawful and setting it aside—would alleviate the administrative and operational costs and burdens the rule places on NRWA's members, including Davidson Water, District #2, Clinton, District #4, and Mahaska, and more than 15,000 other public water systems. It would also alleviate the increased risk of a member system being stuck with a finding of significant deficiency, as well as the risk of increased cybersecurity attack due to public disclosure of sensitive cybersecurity information, that the Rule creates for some members.

48. Because EPA has improperly treated the Cybersecurity Rule as an interpretive rule, NRWA, like other interested parties, has thus far not been afforded a formal opportunity to raise its comments regarding any concerns about the Cybersecurity Rule, such as those described herein, pursuant to APA notice and comment. As such, NRWA has not been afforded the opportunity to protect its members' interests in avoiding excessive, ineffective, potentially harmful, or unlawful regulatory obligations through a fair and transparent regulatory process.

49. If EPA is required to instead promulgate cybersecurity requirements for public water systems through the APA's notice and comment rulemaking process,

then NRWA will have the opportunity to participate in the rulemaking process and provide specific feedback on EPA's proposed requirements and proposed implementation timeline. NRWA intends to participate in any such future rulemaking process.

50. Our members have many years of experience with both sanitary surveys and cybersecurity, and they believe that using sanitary surveys will be ineffective at improving cybersecurity at water systems. As part of our mission to advocate for small and rural water systems, NRWA is committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based and tailored to the particular operational needs and constraints of public water systems. NRWA recognizes 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 those water utilities that will ultimately be subject to sanitary surveys, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector than the one imposed by EPA through the Cybersecurity Rule.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 15th day of May 2023.



Matthew Holmes
Chief Executive Officer
National Rural Water Association

Exhibit C

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF MARK PEPPER

I, Mark Pepper, swear or affirm under penalty of perjury, the following:

1. I am Executive Director for the Wyoming Association of Rural Water Systems (“WARWS”) and have served in this role since 2006. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21, and am competent to make this Declaration.

2. Among other things, my responsibilities as Executive Director of WARWS include: lead advocate for members and public water systems in Wyoming on regulatory and legislative issues. I am also point of contact for State and Federal Agencies looking for background and or outreach on or to Wyoming’s public water

systems, legislators, regulatory personnel or other elected officials of Wyoming’s public water systems. I am a gubernatorial appointee representing governmental entities to the Small System Task Force, The State Emergency Response Commission, the State Non-Point Source Task Force and the State Qualifications Committee. Each of these allow me to adequately express the views and needs of public water systems (“PWSs”) as it relates to each task force, commission or committee.

3. WARWS, established in 1989, is a member-driven, nonprofit association representing all (778) PWSs in the State of Wyoming subject to the Safe Drinking Water Act (“SDWA”) and/or the Clean Water Act. Of the 778 systems, 320 are owned and operated by governmental entities. The remainder are generally owned and operated by private companies or state and federal agencies such as the U.S. Forest Service, National Park Service or State Parks and Recreation. All 778 are subject to sanitary surveys and are required to address deficiencies. WARWS’s mission is “[t]o provide the assistance necessary to meet the needs of our membership and to ensure the protection of Wyoming’s water—our most precious resource. By providing on-site, one-on-one technical assistance and training we can help community elected officials and operators with their commitment and their profession of providing ‘Quality on Tap!’” *See About Us*, Wyo. Ass’n of Rural Water Sys., <https://tinyurl.com/53wnwn9w> (last visited May 5, 2023). WARWS

organizes and runs training programs for Wyoming water and wastewater professionals, allowing them to maintain licensure requirements or prepare for licensure exams, and our “Circuit Rider” program provides on-site, hands-on training and assistance for our member systems on a variety of topics, including water system operation and maintenance, recordkeeping, water quality testing, governance and financial concerns.

4. WARWS is a Wyoming incorporated non-profit and is Wyoming’s state affiliate for the National Rural Water Association (“NRWA”), which operates through a series of state affiliates across the nation. By virtue of this relationship, WARWS’s member systems are members of NRWA through WARWS, and our member systems often attend WARWS state conferences and meetings, as well as those organized by NRWA. Our members also participate in NRWA-run training programs and help represent NRWA as part of its legislative advocacy efforts, such as through NRWA’s “Water Rallies.” A member of WARWS’s Board of Directors represents Wyoming on the NRWA Board of Directors. Currently, the National Director for Wyoming is Chuck McVey, Utility Supervisor from the Town of Saratoga, Wyoming, with a population of approximately 1,700.

5. WARWS’s membership includes PWSs serving over 3,300 people (34 PWSs) that are subject to the cybersecurity requirements in America’s Water Infrastructure Act of 2018 (“AWIA”). WARWS’s membership also includes PWSs

serving fewer than 3,300 people (744 PWSs) that are not subject to the cybersecurity requirements in AWIA. It is our understanding that all PWSs will be subject to the United States Environmental Protection Agency’s (“EPA” or the “Agency”) rule for cybersecurity in sanitary survey’s or alternative process regardless of population or ownership.

6. As PWSs, our member systems are required to comply with the SDWA and EPA implementing regulations.

7. Because Wyoming has neither applied for nor received authority to administer the SDWA within the state, EPA Region 8 has been designated by the EPA to directly implement the SDWA in the State of Wyoming, and its over 775 PWSs. EPA Region 8 is therefore responsible for administering sanitary surveys of PWSs within the State of Wyoming. Wyoming’s PWSs, including WARWS’s member systems, are thus directly regulated by EPA Region 8 when it comes to sanitary surveys. These sanitary surveys are conducted every 3–5 years.

8. I am familiar with EPA’s March 3, 2023 memorandum entitled “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process” (“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises EPA’s interpretations of its SDWA regulations regarding sanitary surveys of PWSs. The revisions require sanitary surveys to include evaluation of a PWS’s cybersecurity systems and controls. I am also familiar with the accompanying

guidance document, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance”), available at <https://tinyurl.com/bdfhfrdj>.

9. WARWS’s membership includes PWSs that use industrial control systems or other operational technology as part of the equipment or operation of a required component of the sanitary survey.

10. Despite creating new regulatory obligations for PWSs, it is my understanding that neither the Cybersecurity Rule nor the Cybersecurity Guidance were subject to the notice-and-comment procedures provided by the Administrative Procedure Act (“APA”).

11. As Executive Director for WARWS, I am generally familiar with EPA Region 8’s implementation of the SDWA in the State of Wyoming, including its sanitary survey program. A sanitary survey is basically an on-site review of a system’s water source, facilities, equipment operations and maintenance in order to evaluate its adequacy to produce and distribute safe drinking water. As part of a sanitary survey of a Wyoming PWS, the inspecting officials (i.e., EPA Region 8 officials or contractors who may not be versed in all aspects of cyber- and physical security issues) are tasked with identifying any “significant deficiencies”—meaning defects, failures, malfunctions, or similar deficiencies—that are causing or have the potential to cause the introduction of contamination into drinking water delivered to

customers. EPA Region 8 must then exercise its authority to require a PWS to address any identified significant deficiencies, regardless of cost/benefit or before employing cost/benefit analysis to the identified deficiency.

12. From working with WARWS's members, I know that the risk of a finding of significant deficiency poses a serious concern for many of our PWS members. Our members therefore often take proactive steps in advance of a sanitary survey to avoid such findings. Members frequently express concern that a findings of significant deficiency, which are generally made public to customers, risk eroding customer confidence in drinking water quality due to the lack of knowledge of the general public to regulatory issues and the inherent risk of misinterpretation to public health of a particular regulatory issue, on top of the possibility of monetary fines or other corrective action directed by EPA Region 8. Members are additionally concerned that the public data (significant deficiency) that may arise about cyber- and physical security of a PWS may unnecessarily alarm citizens regarding the safety of their drinking water supply.

13. The Cybersecurity Rule and the Cybersecurity Guidance, as I understand it, identify a checklist of 36 cybersecurity controls of varying complexity and cost that EPA strongly recommends regulators (who may not be familiar with internal manufacturers controls or general cybersecurity issues) look for during a sanitary survey of a PWS. The Cybersecurity Rule and Guidance further state that

the absence (or inadequacy) of one or more of those controls could be deemed a “significant deficiency” that would require correction by the PWS.

14. The Cybersecurity Rule states that “EPA’s interpretation clarifies that the regulatory requirement to review the ‘equipment’ and ‘operation’ of a PWS necessarily encompasses a review of the cybersecurity practices and controls needed to maintain the integrity and continued functioning of operational technology of the PWS that could impact the supply or safety of the water provided to customers.” Because EPA Region 8 directly administers the SDWA and the sanitary survey program in the State of Wyoming, we and our members can reasonably expect that EPA will apply this interpretation, as further explained in the Cybersecurity Guidance, during upcoming sanitary surveys. As a result, the cost and burdens associated with the Cybersecurity Rule will be directly imposed by EPA.

15. To the extent EPA’s direct implementation of the new cybersecurity requirements differs from the Cybersecurity Guidance, EPA is creating concern and uncertainty among our members by announcing a new “interpretation” of their existing requirements without specifying how they will apply that interpretation to our members and thus increasing their risk of facing a “significant deficiency” in their upcoming sanitary surveys. WARWS is therefore expending time and staff resources to understand the Cybersecurity Rule and the Cybersecurity Guidance, to communicate with members regarding how these requirements differ from their

existing requirements, and to try to better understand how EPA will implement these new requirements.

16. WARWS, like NRWA, believes that cybersecurity is mission-critical for all types of water utilities, especially those in small and rural communities that can be more vulnerable to service disruptions. As such, we support efforts to strengthen cybersecurity as we did with AWIA, and those member systems that were required to address cyber- and physical security per the act and are eager to collaborate with EPA to develop and implement effective approaches for all PWSs. And WARWS is actively involved in assisting its PWS members in evaluating, addressing, and managing cybersecurity risks. EPA's decision, however, to add cybersecurity requirements to the sanitary survey program for drinking water is unlikely to meaningfully improve system resiliency and may ultimately be counterproductive to that goal and harm our members and their customers.

17. In response to the AWIA, WARWS engaged with its member PWSs to assist them in understanding cyber- and physical security needs regardless of population size, conducting training seminars and onsite evaluations of operational control systems and or informational control systems throughout the AWIA implementation timeframe from 2018–2021. We continue to perform these training and awareness sessions. We anticipate doing the same for the new requirements contained in the Cybersecurity Rule, expending our resources and time in the

process. This direct engagement is necessary given the complexity of some of the controls listed by EPA and the understanding gained during the AWIA effort to bridge technology terminology with operational terminology, as well as the reality that the vast majority of our member PWSs do not have full-time, dedicated operational technology (“OT”) and information technology (“IT”) professionals or access to same, as those OT/IT professionals typically demand high salaries due to their expertise and certifications, and due to the small customer base, those professionals are not in great supply to accommodate the needs of this new proposed rule to be able to address any identified issues within reasonable corrective timelines, which may cause undue hardship, misinterpretation and confusion to the populace.

18. Our PWS members will also likely incur initial monetary and time costs in order to understand the Cybersecurity Rule’s requirements as it relates to their particular systems and industry, as well as providing training to staff regarding the new rule’s requirements. Finding cyber professionals who can assist with training and have an understanding of the industry will also cause undue potential costs.

19. WARWS has also consulted with its members to discuss the likely costs and burdens associated with the Cybersecurity Rule and Guidance. Some of our system members have indicated that, while they have cybersecurity systems and controls in place, those measures are focused on their particular operational needs, and do not perfectly align with EPA’s 36-point checklist of cybersecurity controls,

including the 16 control identified by EPA as “potential significant deficiencies” if they are not in place. Those members indicate that they will need to expend money and labor hours to fully understand any perceived discrepancies and implement the listed controls they currently lack so that they can avoid a finding of significant deficiency during their next sanitary survey.

20. Other members have indicated the need to conduct additional cybersecurity assessments and audits on top of the prior assessments they have voluntarily conducted, or conducted pursuant to the AWIA, to determine the extent to which their existing cybersecurity systems conform to EPA’s checklist, including for the 16 potential significant deficiencies. These assessments and audits can be costly and time-consuming, which is likely to be the case with respect to the Cybersecurity Rule and the Cybersecurity Guidance, given the number of cybersecurity controls the Agency has identified. Moreover, cybersecurity assessments do not always produce actionable recommendations unless the cybersecurity professionals conducting the assessments have a firm grasp of the operations of PWSs.

21. Still other members, especially those with limited budgets, have voiced concerns with finding qualified, experienced, yet affordable cybersecurity professionals who can provide clear and actionable recommendations as to how to update their cybersecurity systems. The difficulty in finding, and the cost in hiring,

competent cybersecurity professionals to timely address deficiencies will likely become worse, given the increase in demand for such professionals brought on by the Cybersecurity Rule.

22. Lastly, there is the concern that any cybersecurity-related significant deficiencies recorded during a sanitary survey must be included in a system's "consumer confidence report," and thus made publicly available to its customers. Public identification of potential cybersecurity-related deficiencies could make a PWS a potential target for a cyberattack that disrupts service or threatens water quality. Further, there is concern that cybersecurity-related records submitted to EPA Region 8 could be subject to the Freedom of Information Act, eliminating a system's control over those sensitive documents and increasing the risk of cyberattack, as was the result of the earlier attempts in the early 2,000's with vulnerability assessments and emergency response plans. It is our understanding that that was the impetus for not having AWIA-required assessments or emergency response plans communicated in writing to the Agency, just acknowledgement of completion. Sanitary surveys, by rule, are public documents.

23. WARWS and its members will not incur the above-described costs and burdens associated with the Cybersecurity Rule if the rule is found unlawful and set aside.

24. Because EPA did not provide an APA notice and comment period for the Cybersecurity Rule prior to finalizing the rule, WARWS was unable to use the public comment period as an avenue to express its views and concerns (including through NRWA) and ensure that the Agency would take them into consideration before finalizing this rule.

25. Because EPA did not provide an APA notice and comment period for the Cybersecurity Rule prior to finalizing the rule, WARWS did not have advanced notice about the new requirements in the Cybersecurity Rule and the Cybersecurity Guidance and was therefore not able to engage with EPA Region 8 and WARWS members in advance of the rule being finalized to help ensure that WARWS members were/are prepared for the new requirements.

26. If EPA is required to instead promulgate cybersecurity requirements for public water systems through the APA's notice and comment rulemaking process, then WARWS will have the opportunity to participate in the rulemaking process and provide specific feedback on EPA's proposed requirements and proposed implementation timeline. WARWS will also have the opportunity to prepare its members for the new requirements before they become effective. WARWS intends to participate in any such future rulemaking process directly or through NRWA.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 9th day of May 2023.

A handwritten signature in blue ink that reads "Mark Pepper". The signature is written in a cursive style and is positioned above a horizontal line.

Mark Pepper
Executive Director
Wyoming Association of Rural Water
Systems

Exhibit D

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF ROBERT J. WALTERS

I, Robert J. Walters, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.

2. I am the Vice President, Construction & Engineering and Operator in Responsible Charge (“ORC”) of Davidson Water, Inc. (“Davidson Water”). I have served in this role since 2013. Previously, and since 1985, I held the position of Assistant Manager of Davidson Water.

3. In addition to my roles at Davidson Water, I have been appointed by the Governor of North Carolina to serve on the North Carolina Water Operator Certification Board, where I served for eight years as an appointee and for three years as Chairman.

4. I am certified as a Class A water distribution operator and a cross-connection control operator.

5. Davidson Water is a private, non-profit cooperative water utility headquartered in Lexington, NC that has 66,000 connections, 1,900 miles of water line, and serves drinking water to a population of about 150,000 in seven different cities or towns and across three counties in the middle of North Carolina.

6. Davidson Water is a member of the American Water Works Association (“AWWA”) and the National Rural Water Association (“NRWA”) through its membership in the North Carolina Rural Water Association. Davidson Water relies on AWWA and NRWA to help advocate for its interests, including in rulemakings and in cases such as this one.

7. As Vice President, Construction & Engineering and ORC, I oversee all activities related to drinking water distribution for the Davidson Water service area including those involving compliance with the federal Safe Drinking Water Act (“SDWA”) as well as state law. As a result, I follow new developments in the law, including changes issued by either the U.S. Environmental Protection Agency (“EPA”) or the State of North Carolina’s Department of Environmental Quality (“NC DEQ”). I also provide feedback to

the federal and state government, including through AWWA and NRWA to ensure that Davidson Water's concerns are raised and its interests are protected.

8. As part of my responsibilities, I am involved in Davidson Water's decision-making about how to prepare for sanitary surveys and our cybersecurity practices. As Vice President, Construction & Engineering and ORC, I am also actively involved in other aspects of Davidson Water's operations, including financial, utility management, field operations, and construction.

9. I am familiar with EPA's March 3, 2023, memorandum entitled "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process" ("Cybersecurity Rule"), available at <https://tinyurl.com/mswu6xch>, which revises EPA's interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems ("PWSs") to include evaluations of a system's cybersecurity measures as part of a survey. I know that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related "significant deficiency"—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

10. I am also familiar with EPA guidance accompanying the Cybersecurity Rule, entitled "Evaluating Cybersecurity During Public Water System Sanitary Surveys" ("Cybersecurity Guidance"), available at <https://tinyurl.com/bdfhfrdj>. I am aware that

Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing things like account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

11. I also know that section 7.0 of the Cybersecurity Guidance tells utilities that if they are missing a particular cybersecurity control contained in the checklist, it is a potential significant deficiency. These control measures include, as examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations in evaluating vendors and/or service providers.

12. I understand that the NC DEQ, through the Public Water Supply Section (“PWSS”), administers the SDWA and as part of those responsibilities conducts a sanitary survey our public water system every 3 years. As a public water system, Davidson Water is already subject to periodic sanitary surveys conducted by NC DEQ’s PWSS and will continue to be subject to future sanitary surveys.

13. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements apply to Davidson Water now and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

14. Before NC DEQ's PWSS conducts a sanitary survey, Davidson Water takes steps to avoid a finding of a significant deficiency. We try to avoid any significant deficiencies because they can be costly to correct and they can undermine the confidence of our customers in our practices because the findings are made public. A finding of a significant deficiency causes financial and reputational harm to Davidson Water and community loss of confidence.

15. As far as I am aware, NC DEQ's PWSS has not previously conducted cybersecurity evaluations as part of its sanitary surveys of Davidson Water because cybersecurity evaluations have not been required under EPA's regulations for sanitary surveys. As a result, Davidson Water has not previously faced the risk of a "significant deficiency" as a result of any of its cybersecurity practices.

16. Davidson Water is directly subject to our state's implementation of the new cybersecurity evaluation requirements under EPA's Cybersecurity Rule and Guidance. Because the Cybersecurity Rule says that "states must do the following to comply with the requirement to conduct a 'sanitary survey'" and if "the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the public water system to address the significant deficiency" we understand that the Cybersecurity Rule and Guidance applies directly to us.

17. Davidson Water uses an industrial control system (“ICS”) or other operational technology as part of the equipment or operation of some required components of the sanitary surveys.

18. While Davidson Water does have measures in place to address cybersecurity concerns, those measures do not align with all of the specific requirements outlined in EPA’s Cybersecurity Guidance. Davidson Water’s current cybersecurity measures are instead tailored to its specific operational needs and to complying with America’s Water Infrastructure Act of 2018 (“AWIA”). Davidson Water has recently undertaken a detailed AWIA risk and resiliency assessment of its cybersecurity practices, which included the use of a consultant. I would estimate that our costs of complying with the AWIA requirements will be between \$800,000-900,000.

19. Because the Cybersecurity Rule says that it “significantly builds upon the public health protections in AWIA” we understand that the Cybersecurity Rule has requirements beyond what is required by AWIA, and that we will therefore have to undertake additional measures beyond what we have already done to comply with AWIA.

20. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA as potential significant deficiencies in section 7.0 of the Guidance (“Cybersecurity Checklist”). We will need to spend staff and potentially consultant time to evaluate how to incorporate these requirements into

operations and our annual budget and to understand how they differ from our existing practices or our AWIA resiliency risk assessment plans.

21. Some of the items listed in EPA’s Cybersecurity Checklist of “significant deficiencies” will take meaningful lead time to implement, particularly given how we budget. As a result, Davidson Water cannot afford to wait and see whether NC DEQ’s PWSS adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential significant deficiencies. Instead, Davidson Water must begin spending money and time now to become familiar with the new requirements and act to avoid EPA’s list of significant deficiencies.

22. Davidson Water has already spent time, money, and energy to review the new requirements contained in EPA’s Cybersecurity Rule and Guidance, and will have to expend additional staff time, and likely the time of existing or new IT consultants, to develop a plan to implement the EPA’s new requirements.

23. Based on preliminary look at our existing cybersecurity controls as compared to those listed in the Cybersecurity Checklist, there are at least a few controls that Davidson Water does not presently have in place and/or that will pose operational challenges on Davidson Water.

24. For example, we have already worked with existing IT staff to evaluate compliance with EPA’s Cybersecurity Rule. Through these initial conversations, we have determined that several of the thirty-six items on EPA’s checklist, including items

identified by EPA as potential significant deficiencies, will be difficult for us to implement, including prohibiting the connection of unauthorized hardware such as USB devices, and adhering to the vague encryption recommendations, which may not align with our current encryption practices.

25. Because EPA's Cybersecurity Rule and Guidance tell states to look for particular cybersecurity controls, including those highlighted above, and identifies those controls as potential "significant deficiencies," *see* Cybersecurity Guidance, at 11–14, Davidson Water will need to change its operations and potentially make capital investments to change existing cybersecurity controls and implement new controls before Davidson Water's next sanitary survey to avoid any potential finding of significant deficiency.

26. Davidson Water estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be increased.

27. Because the Cybersecurity Rule was made immediately effective, Davidson Water did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for Davidson Water.

28. Because Davidson Water is a private non-profit co-op, additional costs like those stemming from the Cybersecurity Rule are passed on to our members in the form of

higher rates. Because the Cybersecurity Rule was made immediately effective, Davidson Water did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, and we were unable to make smaller incremental increases to our rates or otherwise communicate the changes to our customers, which harms our relationship with those customers.

29. If NC DEQ's PWSS requires additional, more restrictive, or different cybersecurity controls as a result of EPA's Cybersecurity Rule and Guidance, we will likely need to incur additional internal labor, contractor, and/or capital costs. And given the lead time necessary to implement some cybersecurity measures, Davidson Water will likely need to act early to assess and update its cybersecurity controls and systems prior to its next sanitary survey, rather than wait for the state to implement these different requirements.

30. In order to prepare for sanitary surveys, Davidson Water spends time and money assembling documents that will be reviewed as part of the survey.

31. For future sanitary surveys under the Cybersecurity Rule, Davidson Water will incur additional monetary and internal labor costs to assemble a complex set of documents and records to demonstrate that we comply with the new Cybersecurity Rule requirements. Because Davidson Water has not previously needed to do this work prior to a sanitary survey, the necessary document and data collection and authentication processes

are not presently in place and would need to be created from scratch, requiring Davidson Water to incur additional monetary and internal labor costs.

32. Davidson Water, which operates with 85 total employees, does not presently have on its payroll a cybersecurity expert to manage and review the type of cybersecurity operations in EPA's rule. In order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, Davidson Water will likely need to spend money to either hire a cybersecurity expert or hire a contractor to do similar work. The demand for cybersecurity experts will make it difficult for Davidson Water to hire one without changes to its budget.

33. In the meantime, the burden of evaluating EPA's Cybersecurity Rule will fall on Davidson's Water existing IT staff. By addition these additional duties to our existing staff, the Cybersecurity Rule harms our ability to focus our staff time and resources on the IT and cybersecurity concerns that we find most important to our operations.

34. The Cybersecurity Rule lays out three options for States in including cybersecurity in public water system sanitary surveys. Regardless of whether the State of North Carolina (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require Davidson Water to expend time, money, and

resources in order to assess or prepare in advance of a sanitary survey or alternative State program assessment. Davidson Water will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

35. Davidson Water, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

36. Additionally, while the Cybersecurity Rule proposes to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, Davidson Water has concerns with an approach that puts information about its potential cybersecurity gaps in a centralized database outside of Davidson Water's control.

37. Under EPA regulations, a community water system, like Davidson Water must list in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state's satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule states that cybersecurity gaps are potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our system vulnerable to hackers or similar bad actors who can exploit potential cybersecurity gaps.

38. Even if NC DEQ's PWSS can confidentially protect significant deficiencies or other cybersecurity information, hackers or similar bad actors may still target the state's

database to get information regarding potential cybersecurity vulnerabilities across the state. By centralizing potentially harmful information about a system's vulnerability, the Cybersecurity Rule therefore places Davidson Water at greater risk of a cyberattack. We are also concerned that EPA's regulations may require NC DEQ's PWSS to turn over information about our sanitary surveys to EPA, which would create even more risk that it becomes disclosed.

39. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act ("APA") that would have provided Davidson Water with an opportunity to raise these concerns with the requirements through the notice and comment process. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant to the APA, Davidson Water either independently or through AWWA or NRWA would have raised its concerns including those described above, for EPA's consideration.

40. As a water utility subject to the SDWA, Davidson Water has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect its interests and provide EPA with industry insight and experience.

41. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, Davidson Water would have had more advanced notice of the likely requirements in the rule, which would have assisted Davidson Water in budgeting and

planning accordingly. In addition, because most regulations issued under APA procedures allow some time before going into effect, Davidson Water would have had additional time to prepare for the implementation of the requirements.

42. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA's compliance with notice and comment procedures required by the APA, Davidson Water, a member of AWWA and NRWA, will not face the expected costs associated with complying or failing to comply with EPA's modified regulatory requirements under the Cybersecurity Rule.

43. While Davidson Water will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA's Cybersecurity Guidance as potential "significant deficiencies" if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 12th day of May 2023.

A handwritten signature in black ink, appearing to read 'R. Walters', is positioned above a horizontal line.

Robert J. Walters

Exhibit E

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF CYNTHIA LANE

I, Cynthia Lane, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.
2. I am General Manager of the Platte Canyon Water and Sanitation District (“Platte Canyon”). I have served in this role since 2021. Previously, I held the position of Assistant Manager at Platte Canyon for four years. Prior to joining Platte Canyon, I held the positions of Director of Engineering and Technical Services, Senior Manager of Technical Programs, and Regulatory Engineer with the

American Water Works Association (“AWWA”) for about 5 years, 1 year, and 3 years, respectively.

3. I have a Bachelor of Science degree in Civil Engineering from Pennsylvania State University, which I received in 1999, and a Master of Environmental Engineering from Johns Hopkins University, which I received in 2003. I am also a registered professional engineer in the State of Maryland.

4. Platte Canyon is a quasi-municipal corporation headquartered in Littleton, Colorado, and governed pursuant to provisions of the Colorado Special District Act. Through intergovernmental agreements with the Denver Water Board and the City of Littleton, Platte Canyon provides drinking water distribution and wastewater collection services, respectively, for approximately 6,900 residences and business in eastern Jefferson and western Arapahoe Counties, Colorado. Platte Canyon owns and maintains those water distribution and wastewater collection systems.

5. Platte Canyon is a member of AWWA and relies on AWWA to help represent its interests, including in EPA rulemakings and in cases such as this one.

6. In my capacity as General Manager, I am required to oversee all activities related to drinking water distribution for Platte Canyon’s service area including those involving compliance with the federal Safe Drinking Water Act (“SDWA”) as well as state law. As a result, I follow new developments in Platte

Canyon’s compliance obligations issued by either the U.S. Environmental Protection Agency (“EPA”) or the State of Colorado. I also provide feedback to these entities, including through AWWA, to ensure that Platte Canyon’s concerns are raised and its interests are protected.

7. As part of my responsibilities, I am involved in Platte Canyon’s decision-making about how to prepare for sanitary surveys and our cybersecurity practices. As General Manager, I am also actively involved in other aspects of Platte Canyon’s operations, including financial, board management, field operations, customer communication, intergovernmental relationships, and construction.

8. I am familiar with EPA’s March 3, 2023, memorandum entitled “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process” (“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises EPA’s interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems (“PWSs”) to include evaluations of a system’s cybersecurity measures as part of a survey. I am aware that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related “significant deficiency”—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

9. I am also familiar with the EPA guidance document accompanying the Cybersecurity Rule, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance” or “Guidance”), available at <https://tinyurl.com/bdfhfrdj>. I am aware that Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing general areas of concern including account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

10. I am also aware that section 7.0 of the Cybersecurity Guidance provides that the lack of or inadequacy of a particular cybersecurity control contained in the checklist is a potential significant deficiency. These control measures include, as examples, the PWS maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers.

11. I understand that the State of Colorado administers the SDWA within its borders and as part of those responsibilities the State of Colorado conducts a sanitary survey of our PWS every 3 years. As a PWS, Platte Canyon is already

subject to periodic sanitary surveys conducted by the State of Colorado and will continue to be subject to future sanitary surveys.

12. Platte Canyon uses an industrial control system (“ICS”) or other operational technology as part of the equipment or operation of a required component of the sanitary surveys.

13. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements apply to Platte Canyon now and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

14. Platte Canyon takes steps in advance of the sanitary surveys to avoid a finding that there is a significant deficiency in any of its practices. We seek to avoid any significant deficiencies because they can be costly to correct and they can undermine the confidence of our customers in our practices because the findings are made public. A finding of a significant deficiency therefore causes both financial and reputational harm to Platte Canyon.

15. As far as I am aware, the State has not previously conducted cybersecurity evaluations as part of its sanitary surveys of Platte Canyon because such evaluations have not been required under EPA’s regulations. As a result, Platte Canyon has not previously faced the risk of a “significant deficiency” as a result of any of its cybersecurity practices.

16. Platte Canyon is directly subject to Colorado’s implementation of the new cybersecurity evaluation requirements under EPA’s Cybersecurity Rule and Guidance. Because the Cybersecurity Rule states that “states must do the following to comply with the requirement to conduct a ‘sanitary survey’” and “[i]f the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency” we understand that the Cybersecurity Rule and Guidance apply directly to us.

17. While Platte Canyon does have measures in place to address cybersecurity concerns, those measures do not align with all of the specific requirements outlined in EPA’s Cybersecurity Guidance. Platte Canyon’s current cybersecurity measures are instead tailored to its specific operational needs.

18. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA as potential significant deficiencies in section 7.0 of the Guidance (“Cybersecurity Checklist”). We are already undertaking discussions on how to best implement these requirements and how to adjust our budget and operations to do so.

19. Some of the items listed in EPA’s Cybersecurity Checklist of “significant deficiencies” will take meaningful lead time to implement, particularly

given the nature of our budgeting. As a result, Platte Canyon cannot afford to wait and see whether the State of Colorado adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential significant deficiencies. Instead, Platte Canyon must begin expending resources now to familiarize itself with the new requirements and to implement measures to avoid EPA's list of significant deficiencies.

20. Platte Canyon has already expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and Guidance, and are in the process of developing a plan to implement the requirements contained therein. Doing so requires the involvement of four of Platte Canyon's staff plus the engagement of an external IT consultant. None of these activities were included in the 2023 budget. As a smaller utility, these types of activities can have a significant financial impact as Platte Canyon's annual IT project budget is approximately \$14,000. Platte Canyon estimates that \$4,500 has already been expended to evaluate the new requirements and an additional \$15,000 of staff time, consultant fees, and software implementation will be expended to comply. As the 2024 budget development process is about to commence, it is imperative the total cost of compliance is known now so those values can be budgeted for in future years. A budget overrun, as Platte Canyon is likely to experience this year due to these unplanned compliance expenses, requires public notification and board approval of

a supplemental budget appropriation (per state statute). Platte Canyon has not approved any supplemental budget appropriations in recent years.

21. Based on a preliminary examination of our existing cybersecurity controls as compared to those listed in the Cybersecurity Checklist, there are at least a few controls that Platte Canyon does not presently have in place. For example, Platte Canyon does not maintain an updated inventory of all OT and IT assets, nor an updated configuration of critical OT and IT assets, nor an updated documentation describing network topology across its OT and IT networks. For another, Platte Canyon does not actively integrate cybersecurity considerations as part of its evaluation processes for procurement of OT assets and services. Any further, more intensive audit of Platte Canyon's cybersecurity systems to determine conformance or nonconformance with the Cybersecurity Rule will likely incur additional internal labor and/or contractor costs.

22. Because EPA's Cybersecurity Rule and Guidance instructs states to look for particular cybersecurity controls, including those highlighted above, and identifies those controls as potential "significant deficiencies," *see* Cybersecurity Guidance, at 11–14, Platte Canyon will need to make capital investments to enhance existing cybersecurity controls and implement new ones in anticipation of Platte Canyon's next sanitary survey to avoid any potential finding of significant deficiency.

23. For example, as noted above, EPA’s Cybersecurity Guidance identifies as “potential significant deficiencies”: (1) “PWS does not include cybersecurity requirements and questions in its procurement documents for OT assets and services, which are then evaluated as a part of vendor selection” and (2) “PWS does not stipulate in its procurement documents that vendors and/or service providers shall notify the PWS of security incidents and confirmed vulnerabilities in a timely manner.” These requirements, at a minimum, require Platte Canyon to expend time and resources reviewing its current procurement contracts and could require Platte Canyon to attempt to renegotiate the terms of existing procurement contracts.

24. Platte Canyon estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be doubled, at the very least. For a relatively small PWS like Platte Canyon providing service to less than 7,000 residences and businesses, such an increase in cost would be significant to our budget.

25. Because the Cybersecurity Rule was made immediately effective, Platte Canyon did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for Platte Canyon.

26. In many instances, additional costs like those stemming from the Cybersecurity Rule are passed on to our customers in the form of higher rates.

Because the Cybersecurity Rule was made immediately effective, we were unable to make smaller incremental increases to our rates this year, or otherwise communicate the changes to our customers, which harms our relationship with those customers. Also, if Platte Canyon has to request a supplemental budget appropriation, this likely harms our reputation as it could raise concerns among our customers that our budget development process is flawed.

27. If Colorado requires additional, more restrictive, or differing cybersecurity controls as a result of EPA's Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the lead time necessary to implement some cybersecurity measures, Platte Canyon will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

28. In order to prepare for sanitary surveys, Platte Canyon spends time and money assembling documents that will be reviewed as part of the survey.

29. For future sanitary surveys under the Cybersecurity Rule, Platte Canyon will likely incur significant additional monetary and internal labor costs to assemble a complex set of documents and records to demonstrate its compliance with the applicable cybersecurity review program and to allow the State of Colorado to authenticate Platte Canyon's compliance. Because Platte Canyon has not

previously needed to make such preparations prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would need to be created from scratch, requiring Platte Canyon to incur additional monetary and internal labor costs.

30. Platte Canyon, which operates with fifteen administrative and operations personnel, does not presently have on its payroll a dedicated cybersecurity professional with the requisite qualifications and experience to manage and review the type of cybersecurity operations contemplated under EPA's rule. Thus, in order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, Platte Canyon will likely need to expend money to either hire a dedicated cybersecurity professional or contract with a third party to perform similar cybersecurity services. The demand for qualified personnel capable of performing the work required by the Cybersecurity Rule will make it difficult for Platte Canyon to hire a dedicated employee for this role without changes to its budget.

31. The Cybersecurity Rule lays out three distinct approaches that states should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the State of Colorado (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements

alternative state programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require Platte Canyon to expend time, money, and resources in order to undertake the assessment or prepare in advance of a sanitary survey or alternative state program assessment. Platte Canyon will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

32. Platte Canyon, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

33. Additionally, while the Cybersecurity Rule proposes to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, Platte Canyon has concerns with an approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of Platte Canyon's control.

34. Under EPA regulations, a community water system, like Platte Canyon, must disclose in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state's satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule categorizes cybersecurity gaps as potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our

system vulnerable to targeting by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

35. Even if Colorado is permitted to make deficiencies or other information that it collects related to our cybersecurity practices confidential, there is still the acute risk that a hacker or similar bad actor will target the state's database to obtain information regarding potential cybersecurity vulnerabilities across the state's jurisdiction. By centralizing potentially harmful information about a system's vulnerability, the Cybersecurity Rule therefore places Platte Canyon at greater risk of a cyberattack.

36. Platte Canyon has discussed the Cybersecurity Rule with other PWSs, who have shared similar concerns with the rule and associated guidance.

37. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act ("APA") that would have provided Platte Canyon with an opportunity to raise these concerns with the requirements through the APA's public notice and comment provisions. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant to the APA, Platte Canyon, either independently or through the AWWA, would have raised its concerns, including those described herein, for EPA's consideration.

38. As a regulated entity under the SDWA, Platte Canyon has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and

cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect its interests and provide EPA with industry insight and experience.

39. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, Platte Canyon would have had more advance notice of the likely requirements in the rule, which would have assisted Platte Canyon in budgeting and planning accordingly. In addition, most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded Platte Canyon additional time to prepare for the implementation of the requirements.

40. I am generally familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa (“Petitioners”), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule.

41. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA’s compliance with notice and comment procedures required by the APA, Platte Canyon, a member of AWWA, will not be subjected to the expected costs associated with complying or failing to comply with EPA’s modified regulatory requirements under the Cybersecurity Rule.

42. While Platte Canyon will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA’s

Cybersecurity Guidance as potential “significant deficiencies” if the Cybersecurity Rule is held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 10th day of May 2023.



Cynthia Lane
General Manager
Platte Canyon Water and Sanitation District

Exhibit F

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF FRANK DENNIS OFFUTT

I, Frank Dennis Offutt, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.

2. I am the Executive Director of Public Water Supply District # 4, Platte County, Missouri (“Platte 4 Water”). I have served in this role since 2022. Previously, I held the position of District Manager, Platte 4 Water, for 24 years.

3. I received my Bachelor of Science, Northwest Missouri State University, 1978, Missouri Department of Natural Resources, Certified Operator, #

5187, Class B and DS-III, 1998, and Past Director, Region III, Missouri Rural Water Association, 2015 - 2018.

4. Platte 4 Water (MO1024478) is headquartered in Platte City, MO and serves water to businesses and 8,740 residents across a 39-mile square mile area in central Platte County, MO.

5. Platte 4 Water is a member of National Rural Water Association (“NRWA” # 60438) and the Missouri Rural Water Association (“MRWA” # 308304).

6. In my capacity as Executive Director, I am required to oversee all activities related to drinking water distribution for the Platte 4 Water service area including those involving compliance with the federal Safe Drinking Water Act (“SDWA”) as well as state law. As a result, I follow new developments in Platte 4 Water’s compliance obligations issued by either the U.S. Environmental Protection Agency (“EPA”) or the State of Missouri’s, Department of Natural Resources (“MDNR”). I also provide feedback to these entities through MRWA and NRWA, to ensure that Platte 4 Water’s concerns are raised and its interests are protected.

7. As part of my responsibilities, I am involved in Platte 4 Water’s decision-making about how to prepare for sanitary surveys and our cybersecurity practices. As Executive Director, I am also actively involved in other aspects of

Platte 4 Water's operations, including financial, board management, field operations, and construction.

8. I am familiar with EPA's March 3, 2023, memorandum entitled "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process" ("Cybersecurity Rule"), available at <https://tinyurl.com/mswu6xch>, which revises EPA's interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems ("PWSs") to include evaluations of a system's cybersecurity measures as part of a survey. I am aware that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related "significant deficiency"—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

9. I am also familiar with the EPA guidance document accompanying the Cybersecurity Rule, entitled "Evaluating Cybersecurity during Public Water System Sanitary Surveys" ("Cybersecurity Guidance"), available at <https://tinyurl.com/bdfhfrdj>. I am aware that Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing general areas of concern including account security, device security, governance and training,

vulnerability management, supply chains and third parties, and response and recovery.

10. I am also aware that section 7.0 of the Cybersecurity Guidance provides that the lack of or inadequacy of a particular cybersecurity control contained in the checklist is a potential significant deficiency. These control measures include, as examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers. Platte 4 Water uses an industrial control system (“ICS”) or other operational technology as part of the equipment or operation of some required components of the sanitary survey.

11. I understand that the MDNR administers the SDWA within Missouri borders and as part of those responsibilities conducts a sanitary survey of PWS every 3 years. As a PWS, Platte 4 Water is already subject to periodic sanitary surveys conducted by MDNR and will continue to be subject to future sanitary surveys.

12. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements apply to Platte 4 Water now

and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

13. Platte 4 Water takes steps in advance of the sanitary surveys to avoid a finding that there is a significant deficiency in any of its practices. We seek to avoid any significant deficiencies because they can be costly to correct and they can undermine the confidence of our customers in our practices because the findings are made public. A finding of a significant deficiency therefore causes both financial and reputational harm to Platte 4 Water.

14. As far as I am aware, MDNR has not previously conducted cybersecurity evaluations as part of its sanitary surveys of Platte 4 Water because such evaluations have not been required under EPA's regulations. As a result, Platte 4 Water has not previously faced the risk of a "significant deficiency" as a result of any of its cybersecurity practices.

15. Platte 4 Water is directly subject to MDNR's implementation of the new cybersecurity evaluation requirements under EPA's Cybersecurity Rule and Guidance. Because the Cybersecurity Rule states that "states must do the following to comply with the requirement to conduct a 'sanitary survey'" and if "[MDNR or] the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to

address the significant deficiency” we understand that the Cybersecurity Rule and Guidance applies directly to us.

16. While Platte 4 Water does have measures in place to address cybersecurity concerns, those measures do not align with all of the specific requirements outlined in EPA’s Cybersecurity Guidance. Platte 4 Water’s current cybersecurity measures are instead tailored to its specific operational needs.

17. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA as potential significant deficiencies in section 7.0 of the Guidance (“Cybersecurity Checklist”). We are already undertaking discussions on how to best implement these requirements and how to adjust our budget and operations to do so.

18. Some of the items listed in EPA’s Cybersecurity Checklist of “significant deficiencies” will take meaningful lead time to implement, particularly given the nature of our budgeting. As a result, Platte 4 Water cannot afford to wait and see whether the State of Missouri adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential significant deficiencies. Instead, Platte 4 Water must begin expending resources now to familiarize itself with the new requirements and to implement measures to avoid EPA’s list of significant deficiencies.

19. Platte 4 Water expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and Guidance, and to acquire an understanding for developing a plan to implement the requirements contained therein. Platte 4 Water has made no previous preparation for the Cybersecurity Rule. Platte 4 Water's courtesy review of the EPA Cybersecurity Rule to date has accumulated 26 hours of staff time, and 4 hours of consultant time identifying the scope of service requirements towards becoming compliant. No training of Platte 4 Water's staff has occurred or is scheduled at time. There is no funding identified in Platte 4 Water's FY2023 budget to address the district's compliance with the Cybersecurity Rule. Funding to implement the Cybersecurity Rule will require a new line item in Platte 4 Water's future budget(s). The FY2024 budget process is scheduled to begin, June 2023. A "perfected FY2024 budget document is scheduled for public review" November 6, 2023. Platte 4 Water's Board of Directors are scheduled to consider legislation to adopt the FY2024 Budget, December 14, 2023. Platte 4 Water strives to be without deficiencies in all aspects of material, technical, financial and managerial operations. At present no resources are identified to fund and assure compliance with the Cybersecurity Rule.

20. Based on a preliminary examination of our existing cybersecurity controls as compared to those listed in the Cybersecurity Checklist, there are at least a few controls that Platte 4 Water does not presently have in place. For example, two

primary areas requiring funding for Platte 4 Water to become compliant with the EPA Cybersecurity Rule is training and additional staff. Due to the time constraint, Platte 4 Water is unable to provide a final figure as to the funding required for the district to become compliant with the Cybersecurity Rule.

21. Because EPA’s Cybersecurity Rule and Guidance instruct states to look for particular cybersecurity controls, including those stated previously, and identifies those controls as potential “significant deficiencies,” *see* Cybersecurity Guidance, at 11–14, Platte 4 Water will need to make capital investments to enhance existing cybersecurity controls and implement new ones in anticipation of Platte 4 Water’s next sanitary survey to avoid any potential finding of significant deficiency.

22. Platte 4 Water estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be increased [estimate of \$25k - \$ 40K].

23. Because the Cybersecurity Rule was made immediately effective, Platte 4 Water did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for Platte 4 Water.

24. In many instances, additional costs like those stemming from the Cybersecurity Rule are passed on to our customers in the form of higher rates. Because the Cybersecurity Rule was made immediately effective, Platte 4 Water did

not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, we were unable to make smaller incremental increases to our rates or otherwise communicate the changes to our customers, which harms our relationship with those customers.

25. If MDNR requires additional, more restrictive, or differing cybersecurity controls as a result of EPA's Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the lead time necessary to implement some cybersecurity measures, Platte 4 Water will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

26. In order to prepare for sanitary surveys, Platte 4 Water spends time and money assembling documents that will be reviewed as part of the survey.

27. For future sanitary surveys under the Cybersecurity Rule, Platte 4 Water will likely incur significant additional monetary and internal labor costs to assemble a complex set of documents and records to demonstrate its compliance with the applicable cybersecurity review program and to allow the State of Missouri to authenticate Platte 4 Water compliance. Because Platte 4 Water has not previously needed to make such preparations prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would

need to be created from scratch, requiring Platte 4 Water to incur additional monetary and internal labor costs.

28. Platte 4 Water, which operates with 6 administrative and operations personnel, does not presently have on its payroll a dedicated cybersecurity professional with the requisite qualifications and experience to manage and review the type of cybersecurity operations contemplated under EPA's rule. Thus, in order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, Platte 4 Water will likely need to expend money to either hire a dedicated cybersecurity professional or contract with a third party to perform similar cybersecurity services. The demand for qualified personnel capable of performing the work required by the Cybersecurity Rule will make it difficult for Platte 4 Water to hire a dedicated employee for this role without changes to its budget.

29. The Cybersecurity Rule lays out three distinct approaches that States should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the State of Missouri (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require Platte 4 Water

to expend time, money, and resources in order to undertake the assessment or prepare in advance of a sanitary survey or alternative State program assessment. Platte 4 Water will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

30. Platte 4 Water, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

31. Additionally, while the Cybersecurity Rule proposes to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, Platte 4 Water has concerns with an approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of Platte 4 Water's control.

32. Under EPA regulations, a community water system, like Platte 4 Water, must disclose in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state's satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule categorizes cybersecurity gaps as potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our system vulnerable to targeting by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

33. Even if Missouri is able to make deficiencies or other information that it collects related to our cybersecurity practices confidential, there is still the acute risk that a hacker or similar bad actor will target the state's database to obtain information regarding potential cybersecurity vulnerabilities across the state's jurisdiction. By centralizing potentially harmful information about a system's vulnerability, the Cybersecurity Rule therefore places Platte 4 Water at greater risk of a cyberattack.

34. Platte 4 Water has discussed the Cybersecurity Rule with other PWSs, who have shared similar concerns with the rule and associated guidance.

35. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act ("APA") that would have provided Platte 4 Water with an opportunity to raise these concerns with the requirements through the APA's public notice and comment provisions. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant to the APA, Platte 4 Water, either independently or through the NRWA, would have raised its concerns including those described herein, for EPA's consideration.

36. As a regulated entity under the SDWA, Platte 4 Water has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent

regulatory process to protect its interests and provide EPA with industry insight and experience.

37. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, Platte 4 Water would have had more advanced notice of the likely requirements in the rule, which would have assisted Platte 4 Water in budgeting and planning accordingly. In addition, most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded Platte 4 Water additional time to prepare for the implementation of the requirements.

38. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA's compliance with notice and comment procedures required by the APA, Platte 4 Water, a member of NRWA, will not be subjected to the expected costs associated with complying or failing to comply with EPA's modified regulatory requirements under the Cybersecurity Rule.

39. While Platte 4 Water will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA's Cybersecurity Guidance as potential "significant deficiencies" if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 12th day of May 2023.



Frank Dennis Offutt

STATE OF MISSOURI)
) ss.
COUNTY OF PLATTE)

On this 12th day of May 2023, before me, appeared Frank Offutt to me personally known, who being by me duly sworn, did say that he is Executive Director of PUBLIC WATER SUPPLY DISTRICT # 4, Platte County, Missouri, a political subdivision, that the seal affixed to the foregoing instrument is the official seal of said WATER DISTRICT and that said instrument was signed and sealed in behalf of said Frank Offutt.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed my official seal at my office in the State of Missouri the day and year last above written.



KELLY O'NEILL
My Commission Expires
May 21, 2023
Platte County
Commission #19085023

Notary Public
My term expires:

Exhibit G

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF SCOTT BORMAN

I, Scott Borman, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.

2. I am the General Manager of the Benton Washington Regional Public Water Authority (“BWRPWA”) and have served in this role since 2002. Prior to joining BWRPWA, I was employed as Program Manager for Environmental Health by the Nebraska Department of Health and Human Services for approximately four years, with oversight of the Field Services Division (Sanitary Surveys and Comprehensive Performance Evaluations), Water Operator Certification Program,

and Capacity Development Program for developing Technical, Managerial, and Financial Capacity in water utilities within the state. Before that, as a Utilities Superintendent for the City of Chardon, Nebraska, for about four years. I have a Bachelor of Science degree in Animal Sciences from Colorado State University, which I received in 1984, and have a total of over 31 years of experience in the drinking water operations, management, and regulatory sectors.

3. Founded in 1992, BWRPWA is a public water authority and regional water wholesaler that collects and treats water from the Beaver Lake reservoir in northwest Arkansas for distribution to seventeen municipal and rural systems in northwest Arkansas and eastern Oklahoma, which collectively comprise a service area of approximately 135,000 individual, industrial, commercial, and agricultural customers, including the nation's largest poultry processing plant and the Northwest Arkansas National Airport. BWRPWA owns and operates intake facilities on Beaver Lake; a treatment plant located in Avoca, Arkansas; and an extensive network of transmission mains, storage facilities, and booster pump stations. BWRPWA funds its operations and capital improvements solely through the rates it charges and municipal bond offerings. The rates it charges are subject to approval by BWRPWA's board of directors (the "BWRPWA Board"), which is comprised of representatives from the municipal and rural water systems we serve, and derived from third-party rate studies which take into consideration future capital

improvements and funding needs. Currently, the BWRPWA Board has set those rates through 2025 with additional capital improvement spending through that period.

4. In my capacity as General Manager of BWRPWA, I am required to oversee all activities related to water collection, treatment, and distribution, including all those involving compliance with the Safe Drinking Water Act (“SDWA”), as well as state law. I also work closely with BWRPWA Board on a variety of operational, financial, and construction-related matters by making recommendations to the BWRPWA Board.

5. As part of my responsibilities, I am involved in BWRPWA’s decision-making about how to prepare for state-conducted sanitary surveys, as well as how best to manage our cybersecurity risk and implement appropriate cybersecurity controls. In light of these responsibilities, I follow new developments in BWRPWA’s compliance obligations, including those issued by the U.S. Environmental Protection Agency (“EPA” or the “Agency”) and the State of Arkansas. And I provide feedback to these entities, including through the American Water Works Association (“AWWA”) and its state and regional networks, to ensure that BWRPWA’s concerns are raised for consideration and its interests protected.

6. BWRPWA is a member of AWWA and relies on AWWA to help represent its interests, including in EPA rulemakings and in cases such as this.

7. I am familiar with EPA's March 3, 2023 memorandum entitled "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process" ("Cybersecurity Rule"), available at <https://tinyurl.com/mswu6xch>, which revises EPA's interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems ("PWSs") to now require evaluation of a system's cybersecurity measures as part of a sanitary survey. The Cybersecurity Rule, as I understand it, requires that if a state identifies a cybersecurity-related "significant deficiency" (i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers) as part of a sanitary survey, it must record the significant deficiency in a publicly available record, and require the PWS to address the deficiency.

8. I am also familiar with the guidance document accompanying the Cybersecurity Rule, entitled "Evaluating Cybersecurity During Public Water System Sanitary Surveys" ("Cybersecurity Guidance"), available at <https://tinyurl.com/bdfhfrdj>. The Cybersecurity Guidance, at Section 7, lists 16 potential cybersecurity-related significant deficiencies and provides, at Appendix A, a checklist of 36 cybersecurity controls addressing cybersecurity considerations, such as account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

9. I am also aware that the Cybersecurity Guidance provides that the lack (or inadequacy) of a particular cybersecurity control contained in the Appendix A checklist is a potential significant deficiency. These control measures include, as a few examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers.

10. I am aware that the Cybersecurity Rule and Cybersecurity Guidance were issued and made immediately effective without EPA providing interested parties, like BWRPWA or AWWA, the customary notice-and-comment period.

11. The State of Arkansas conducts sanitary surveys every two years with the last sanitary survey having occurred in December 2021. Since it operates a PWS, BWRPWA is already subject to periodic sanitary surveys conducted by the State of Arkansas and will continue to be subject to future sanitary surveys.

12. Before a sanitary survey, BWRPWA takes steps to avoid Arkansas finding a “significant deficiency.” Not only can significant deficiencies be costly to fix, but the State’s deficiency findings are generally made publicly available, which can undermine the confidence of BWRPWA’s customers in their

water system. In other words, a finding of a significant deficiency can result in both financial and reputational harm to BWRPWA. In addition, because the findings are public documents, a deficiency finding could be used by third parties to determine any specific vulnerability the system may have and subsequently provide a path for it to be compromised.

13. As I understand it, EPA issued the Cybersecurity Rule and Cybersecurity Guidance as immediately effective, meaning that its requirements now apply to the State of Arkansas's sanitary surveys and that BWRPWA's cybersecurity practices will be evaluated by the State during its next annual sanitary survey.

14. BWRPWA uses an industrial control system ("ICS") or other operational technology as part of the equipment or operation of some required components of the sanitary surveys.

15. To the best of my knowledge, the State of Arkansas has not previously conducted cybersecurity evaluations as part of its sanitary surveys of BWRPWA. BWRPWA has therefore not previously faced the possibility of a finding of significant deficiency relate to its cybersecurity practices and systems.

16. BWRPWA is directly subject to Arkansas's implementation of EPA's requirements under the Cybersecurity Rule and Cybersecurity Guidance. The Cybersecurity Rule provides that states "must" "evaluate the adequacy of the

cybersecurity of [the] operational technology [used by a PWS] for producing and distributing safe drinking water.” Cybersecurity Rule, at 2–3. And the rule further requires that “[i]f the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency.” *Id.* As a PWS, BWRPWA understands the Cybersecurity Rule and Cybersecurity Guidance to impose compliance obligations on us.

17. BWRPWA presently has controls in place to address the cybersecurity needs for its water system, and has conducted internal cybersecurity audits to determine areas of improvement and hired competent staff to handle cybersecurity issues that do arise. BWRPWA is also a member of the Water Information Sharing and Analysis Center (“Water ISAC”), a nonprofit “all-threats” security information resource for the water and wastewater sector that frequently collaborates with EPA. Through Water ISAC, BWRPWA receives notices about possible cybersecurity threats so that we may respond accordingly.

18. BWRPWA’s controls, however, are designed to meet its particular operational needs, and thus do not completely align with the six-page list of 36 controls provided in the Cybersecurity Guidance.

19. Given that the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the suite of cybersecurity

controls listed in the Cybersecurity Guidance. To proceed otherwise risks a finding of significant deficiency during our next sanitary survey. We are therefore already undertaking discussions on how to best implement EPA's requirements and how to adjust our budget and operations to do so.

20. Some of the cybersecurity controls listed in EPA's Cybersecurity Guidance will take meaningful lead time to implement because of budgeting and staffing limitations. BWRPWA operates on a calendar fiscal year, meaning annual budgets for expenditures are set in October each year, as well as staffing requirements. Considering salaries, equipment, software and other expenditures, BWRPWA already currently spends approximately \$350,000 per year on cybersecurity and that cost changes annually due to different evolving threats. Because EPA has implemented these rules immediately, that means that BWRPWA does not have the leeway to wait and see whether the State of Arkansas adopts the entire Cybersecurity Guidance checklist before taking steps to implement those items that could form the basis of a finding of significant deficiency. Instead, BWRPWA will need to begin expending resources to both familiarize itself with the requirements of EPA's Cybersecurity Rule and Guidance and implement EPA's suite of cybersecurity controls in order to avoid a finding of significant deficiency.

21. BWRPWA has already expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and Guidance,

and to develop a plan to implement the requirements contained therein. BWRPWA's preliminary review of the required cybersecurity controls will require us to add approximately an additional \$75,000 to \$100,000 in our Fiscal Year 2024 Budget. This is despite the fact that our Bond Rating Agency, S&P, and our insurance carrier, Cincinnati, have deemed our existing cybersecurity controls sufficient during rating reviews and insurance renewals.

22. Based on a preliminary examination of our existing cybersecurity controls as compared to those listed in the Cybersecurity Guidance checklist, there are at least a few controls that BWRPWA does not presently have in place. The major one is concerning integrating cybersecurity evaluations in procurement and supply line contracting. This checklist item is overbearing and unnecessary and will require the cooperation of the individual supply chain vendors that we deal with on a routine basis. These supply chain vendors do not normally fall under EPA rulemaking and consequently have no incentive or need to share that information with BWRPWA. However, if BWRPWA does not have that information, we are subject to a finding of significant deficiency under the checklist. BWRPWA understands the supply chain vendors unwillingness to partake in any cybersecurity evaluations since, under the requirements, as part of the sanitary survey process, the supply chain vendor's cybersecurity practices could be exposed publicly as well. At this time, BWRPWA does not believe that this control requirement can be or should

be implemented because it is technically unfeasible and unnecessary. But at this point, failure to complete will result in a significant deficiency.

23. There may be other differences in the controls BWRPWA has in place and those listed in the Guidance, but a more intensive audit of BWRPWA's cybersecurity systems to determine conformance or nonconformance would mean additional internal labor and/or contractor costs. While there are differences between the EPA's list of requirements and our practices, there are obvious concerns in revealing those differences in this declaration, as making that information public could make BWRPWA a vulnerable target for cyberattack.

24. Because EPA's Cybersecurity Rule and Guidance instruct states to look for particular cybersecurity controls, including those highlighted above, and identify many of those controls as bases for potential significant deficiencies, BWRPWA will need to make capital investments to enhance existing cybersecurity controls and implement new ones before BWRPWA's next sanitary survey to avoid any potential finding of significant deficiency.

25. BWRPWA estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, we will need to spend additional time and money. As stated previously, after preliminary review of the control requirements, our Fiscal Year 2023 (current year) spending would need to increase an additional \$75,000 to \$100,000 to meet all the requirements except one, which is

the supply chain cybersecurity issue, with which we do not believe any water utility will be able to fully comply. This will bring our overall cybersecurity spending to approximately \$450,000 per year in subsequent years and the reality of being fully in compliance with all the requirements very unlikely. As a water wholesaler whose rates are subject to approval by representatives of the municipalities and water districts we serve, these increases in cost are significant. Additional costs, like those required by the requirements in the Cybersecurity Rule, will be passed on to the ultimate customer of our water—individuals, businesses, and agricultural operators.

26. Because the Cybersecurity Rule was made immediately effective, BWRPWA did not have any notice or time to prepare for the new requirements or to forecast the costs into future budgeting plans. The resulting uncertainty regarding rate planning and cost recovery—and the need to communicate any incremental increases in rates to customers—will create additional implementation challenges.

27. If Arkansas requires additional, more restrictive, or differing cybersecurity controls, as compared to EPA’s Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the lead time necessary to implement some cybersecurity measures, as noted above, BWRPWA will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

28. To prepare for sanitary surveys, BWRPWA spends time and money to assemble the documents and records that state inspectors will review as part of the survey. For future sanitary surveys under the Cybersecurity Rule, BWRPWA will likely incur costs (including internal labor costs) to put together the documents and records for the sanitary survey in order to document our compliance with the cybersecurity review program requirements and to allow the State of Arkansas to authenticate BWRPWA's compliance. Because BWRPWA has not previously needed to make these kinds of preparations before a sanitary survey, the necessary document and data collection and authentication processes are not currently in place and would need to be created from scratch. This will require BWRPWA to incur additional monetary and internal labor costs.

29. BWRPWA is a large public water supply, and because of the nature of our system, we are able to have staff that handle all of our cybersecurity needs. We currently have two employees dedicated to handling our data acquisition and cybersecurity. The cost to BWRPWA for these employees, when considering both direct and indirect personnel costs, is \$198,500 for Fiscal Year 2023. However, we are only able to do this because we are a regional system and can apply economies of scale to help spread out this cost to all of our customers equally. This is not true of the small systems to which we provide potable water. These small systems (3,300 to 10,000 served) often rely on third-party vendors to meet all of their IT/OT and

cybersecurity needs. Very often, these are one-person vendors operating out of an office or home and, based on my discussions with some of them, are not even aware of the new cybersecurity requirements with which these small systems will have to comply. Realistically, they do not have the funds, knowledge or staff to implement and meet all these requirements. Furthermore, some of these small systems have been left without records, or system knowledge, when their third-party vendor decides they are no longer in business. Some small utilities cannot even change, add, or delete an email address without going through their third-party vendor. This rule was written and is being implemented as one set of standards that applies to everybody serving over 3,300 customers and ignores the reality of implementing and adhering to all of the cybersecurity requirements mandated for all systems. There is no flexibility or rational weighing of alternative methods of cybersecurity for the smaller systems.

30. The Cybersecurity Rule includes three possible approaches that states should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the State of Arkansas (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require BWRPWA to expend time, money, and resources in order to undertake the assessment or prepare

in advance of a sanitary survey or alternative State program assessment. BWRPWA will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

31. BWRPWA, and ultimately its customers, will face the costs described herein unless the Cybersecurity Rule is found unlawful and set aside.

32. Additionally, while the Cybersecurity Rule claims to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, BWRPWA has concerns with the rule's approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of BWRPWA's control.

33. Under EPA regulations, a community water system, like BWRPWA, must disclose in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if such deficiency is not corrected to the state's satisfaction. In addition, reports from sanitary surveys are submitted to the surveyed PWS, as well as any relevant municipal or government officials. Those records are generally considered public documents under Arkansas law; even if not made publicly available, the records may be subject to the very open and widespread Arkansas Freedom of Information Act. Because the Cybersecurity Rule categorizes cybersecurity gaps as potential significant deficiencies, any gaps identified as part of a sanitary survey would likely be made public, whether by way of consumer

confidence reports or as records made available under open records laws. Not only would public disclosure of cybersecurity-related significant deficiencies undermine customer trust in our water system—even if the system’s cybersecurity measures are strong but do not cover every cybersecurity measure in EPA’s six-page checklist—but also make that system vulnerable to being targeted by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

34. BWRPWA also has concerns about providing copies of cybersecurity documents, like OT and IT inventories and configurations, to State officials. BWRPWA’s existing cybersecurity procedures require maintaining secure control over such documents and limiting outside and inside access. This procedure is designed to limit the availability of information that could be used by nefarious actors to discover and target potential weaknesses in BWRPWA’s systems. That is why when disclosing information about its cybersecurity measures to bond raters and insurance carriers, BWRPWA generally provides a broad overview of its cybersecurity systems and gives specific details only as needed. This control is weakened, however, if comprehensive inventories of BWRPWA’s cybersecurity systems and other sensitive cybersecurity documents are given to outside entities, including State regulators, over which BWRPWA has no control nor assurance of security. In other words, some of EPA’s cybersecurity controls are likely to directly

conflict with BWRPWA's existing cybersecurity controls, namely control of cybersecurity-related documents.

35. Even if Arkansas is able to make deficiencies confidential, there is still a very real risk that a hacker will target the Arkansas's database to obtain information regarding potential cybersecurity vulnerabilities across the state's jurisdiction. By centralizing potentially harmful information about a system's vulnerability, the Cybersecurity Rule places BWRPWA at greater risk of a cyberattack.

36. BWRPWA has discussed the Cybersecurity Rule with other PWSs that have similar concerns with the rule and associated guidance.

37. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided issuing the rule pursuant to formal notice and comment under the Administrative Procedure Act ("APA"). If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant to the APA, BWRPWA, either independently or through the AWWA, would have raised its concerns including those described herein, for EPA's consideration. Previously BWRPWA has provided comments and information through AWWA on the Revised Total Coliform Rule and directly to EPA on the proposed Perchlorate Rule, the newly revised Lead Copper Rule, the current rule revisions being discussed under the Microbial and Disinfection By-Product Rule Revision Workgroup and through being a member of the National Drinking Water Advisory Council.

38. As a regulated entity under the SDWA, BWRPWA has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect those interests and provide EPA with industry insight and experience.

39. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, BWRPWA would have had more advance notice of the likely requirements in the rule, which would have assisted BWRPWA in budgeting and planning accordingly. Most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded BWRPWA additional time to prepare for the implementation of the requirements.

40. I am generally familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa (“Petitioners”), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule.

41. If the court holds the Cybersecurity Rule to be unlawful and sets it aside, pending, at a minimum, EPA’s compliance with notice-and-comment procedures required by the APA, BWRPWA, a member of AWWA, will not be subjected to the expected costs associated with complying or failing to comply with EPA’s modified regulatory requirements under the Cybersecurity Rule.

42. While BWRPWA will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA's Cybersecurity Guidance as potential "significant deficiencies" if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 8th day of May 2023.



Scott Borman
General Manager
Benton Washington Regional Public Water
Authority

Exhibit H

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

**DECLARATION OF Sharon A Cornelius, Public Water Supply District #2
Andrew County**

I, Sharon Cornelius, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.

2. I am the Manager of the Public Water Supply District #2 Andrew County (“PWSD #2”). I have served in this role since 2018. Previously, I held the position of Controller of a Regional Health Care Facility, management of a non for profit, auditing, and tax preparation for public accounting firms.

3. In this role I have completed and received the Missouri Dept of Natural Resources Certificate of Competency Water Distribution level I and have continued

to stay current through continuing education of relevant topics impacting water and water districts. In addition, I have a Bachelor of Science in Accountancy and Finance.

4. PWSD #2 has water connections in five counties with the majority in Andrew and Buchanan County Mo. The district is approximately 300 square miles with approximately 1500 customers and the district office is in Cosby, Mo.

5. I and PWSD #2 are members of National Rural Water Association and Missouri Rural Water Association

6. In my capacity as manager, I am required to oversee all activities related to drinking water distribution for PWSD #2 service area including those involving compliance with the federal Safe Drinking Water Act (“SDWA”) as well as state law. As a result, I follow new developments in PWSD #2 compliance obligations issued by either the U.S. Environmental Protection Agency (“EPA”) or the State of Missouri Department of Natural Resources. I also provide feedback to these entities, including through National Rural Water Association and Missouri Rural Water Association, to ensure that PWSD #2’s concerns are raised, and its interests are protected.

7. As part of my responsibilities, I am involved in PWSD #2’s decision-making about how to prepare for sanitary surveys and our cybersecurity practices.

As manager, I am also actively involved in other aspects of PWSD #2 operations, including financial, board management, field operations, and construction.

8. I am familiar with EPA's March 3, 2023, memorandum entitled "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process" ("Cybersecurity Rule"), available at <https://tinyurl.com/mswu6xch>, which revises EPA's interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems ("PWSs") to include evaluations of a system's cybersecurity measures as part of a survey. I am aware that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related "significant deficiency"—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

9. I am also familiar with the EPA guidance document accompanying the Cybersecurity Rule, entitled "Evaluating Cybersecurity During Public Water System Sanitary Surveys" ("Cybersecurity Guidance"), available at <https://tinyurl.com/bdfhfrdj>. I am aware that Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing general areas of concern including account security, device security, governance and training,

vulnerability management, supply chains and third parties, and response and recovery.

10. I am also aware that section 7.0 of the Cybersecurity Guidance provides that the lack of or inadequacy of a particular cybersecurity control contained in the checklist is a potential significant deficiency. These control measures include, as examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers.

11. I understand that the Missouri DNR administers the SDWA within its borders and as part of those responsibilities conducts a sanitary survey of PWS every three years. As a PWS, Public Water Supply District #2 Andrew County is already subject to periodic sanitary surveys conducted by Missouri DNR and will continue to be subject to future sanitary surveys.

12. Public Water Supply District #2 Andrew County uses industrial control systems or other operational technology as part of the equipment or operation of a required component of a sanitary survey. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements

apply to PWSD #2 Andrew County now and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

13. Public Water Supply District #2 Andrew County takes steps in advance of the sanitary surveys to avoid a finding that there is a significant deficiency in any of its practices. We seek to avoid any significant deficiencies because they can be costly to correct, and they can undermine the confidence of our customers in our practices because the findings are made public. A finding of a significant deficiency therefore causes both financial and reputational harm to Public Water Supply District #2 Andrew County.

14. As far as I am aware, Missouri DNR has not previously conducted cybersecurity evaluations as part of its sanitary surveys of PWSD #2 Andrew County because such evaluations have not been required under EPA's regulations. As a result, PWSD #2 Andrew County has not previously faced the risk of a "significant deficiency" as a result of any of its cybersecurity practices.

15. Public Water Supply District #2 Andrew County is directly subject to Missouri Department of Natural Resource's (DNR) implementation of the new cybersecurity evaluation requirements under EPA's Cybersecurity Rule and Guidance. Because the Cybersecurity Rule states that "states must do the following to comply with the requirement to conduct a 'sanitary survey'" and if Mo DNR determines that a cybersecurity deficiency identified during a sanitary survey is

significant, then the state must use its authority to require the PWS to address the significant deficiency” we understand that the Cybersecurity Rule and Guidance applies directly to us.

16. While PWSD #2 does have measures in place to address cybersecurity concerns, those measures do not align with all the specific requirements outlined in EPA’s Cybersecurity Guidance. PWSD #2’s current cybersecurity measures are instead tailored to its specific operational needs.

17. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA and sixteen listed as potential significant deficiencies in section 7.0 of the Guidance (“Cybersecurity Checklist”). We are already undertaking discussions on how to best implement these requirements and how to adjust our budget and operations to do so. Frankly, these additional requirements are daunting to a rural water district and will put a strain on human and financial resources.

18. Some of the items listed in EPA’s Cybersecurity Checklist of “significant deficiencies” will take meaningful lead time to implement, particularly given the nature of our budgeting. As a result, PWSD #2 cannot afford to wait and see whether the State of Missouri DNR adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential

significant deficiencies. Instead, PWSD #2 must begin expending resources now to familiarize itself with the new requirements and to implement measures to avoid EPA's list of significant deficiencies.

19. PWSD #2 has already expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and Guidance, and to develop a plan to implement the requirements contained therein. This unexpected, unfunded mandate can put a severe strain and stress on personnel in time and financial capacity to implement the requirements of the Cybersecurity Rule Plan. Please reconsider abandoning these new requirements for the severe difficulties it will impose on rural water districts.

20. Because EPA's Cybersecurity Rule and Guidance instruct states to look for particular cybersecurity controls, including those highlighted above, and identifies those controls as potential "significant deficiencies," *see* Cybersecurity Guidance, at 11–14, PWSD #2 will need to make capital investments to enhance existing cybersecurity controls and implement new ones in anticipation of PWSD #2's next sanitary survey to avoid any potential finding of significant deficiency.

21. PWSD #2 estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be increased significantly to educate, identify and implement the requirements.

22. Because the Cybersecurity Rule was made immediately effective, PWSD #2 did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for PWSD #2.

23. In many instances, additional costs like those stemming from the Cybersecurity Rule are passed on to our customers in the form of higher rates. Because the Cybersecurity Rule was made immediately effective, PWSD #2 did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, we were unable to make smaller incremental increases to our rates or otherwise communicate the changes to our customers, which harms our relationship with those customers.

24. If Missouri DNR requires additional, more restrictive, or differing cybersecurity controls because of EPA's Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the lead time necessary to implement some cybersecurity measures, PWSD #2 will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

25. To prepare for sanitary surveys, PWSD #2 spends time and money assembling documents that will be reviewed as part of the survey.

26. For future sanitary surveys under the Cybersecurity Rule, PWSD #2 will likely incur significant additional monetary and internal labor costs to assemble a complex set of documents and records to demonstrate its compliance with the applicable cybersecurity review program and to allow the Missouri DNR to authenticate PWSD #2's compliance. Because PWSD #2 has not previously needed to make such preparations prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would need to be created from scratch, requiring PWSD #2 to incur additional monetary and internal labor costs.

27. PWSD #2, which operates with one administrative and four operations personnel, does not presently have on its payroll a dedicated cybersecurity professional with the requisite qualifications and experience to manage and review the type of cybersecurity operations contemplated under EPA's rule. Thus, to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, PWSD #2 will likely need to expend money to either hire a dedicated cybersecurity professional or contract with a third party to perform similar cybersecurity services. The demand for qualified personnel capable of performing the work required by the Cybersecurity Rule will make it difficult for PWSD #2 to hire a dedicated employee for this role without changes to its budget.

28. The Cybersecurity Rule lays out three distinct approaches that States should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the State of Missouri (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require PWSD #2 to spend time, money, and resources in order to undertake the assessment or prepare in advance of a sanitary survey or alternative State program assessment. PWSD #2 will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

29. PWSD #2, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

30. Additionally, while the Cybersecurity Rule proposes to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, PWSD #2 has concerns with an approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of PWSD #2's control.

31. Under EPA regulations, a community water system, like PWSD #2, must disclose in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state's

satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule categorizes cybersecurity gaps as potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our system vulnerable to targeting by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

32. Even if Missouri DNR is permitted to make deficiencies or other information that it collects related to our cybersecurity practices confidential, there is still the acute risk that a hacker or similar bad actor will target the state's database to obtain information regarding potential cybersecurity vulnerabilities across the state's jurisdiction. By centralizing potentially harmful information about a system's vulnerability, the Cybersecurity Rule therefore places PWSD #2 at greater risk of a cyberattack. PWSD #2 is concerned that risk is even greater if Missouri DNR must also provide information about our cybersecurity practices to EPA.

33. PWSD #2 has discussed the Cybersecurity Rule with other PWSs, who have shared similar concerns with the rule and associated guidance.

34. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act ("APA") that would have provided PWSD #2 with an opportunity to raise these concerns with the requirements through the APA's public notice and comment provisions. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant

to the APA, PWSD #2, either independently or through the National Rural Water Association and Missouri Rural Water Association, would have raised its concerns including those described herein, for EPA's consideration.

35. As a regulated entity under the SDWA, Public Water Supply District #2 Andrew County has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect its interests and provide EPA with industry insight and experience.

36. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, PWSD #2 Andrew County would have had more advanced notice of the likely requirements in the rule, which would have assisted Public Water Supply District #2 Andrew County in budgeting and planning accordingly. In addition, most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded PWSD #2 additional time to prepare for the implementation of the requirements.

37. I am generally familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa ("Petitioners"), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule.

38. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA's compliance with notice and comment procedures required by

the APA, PWSD #2, a member of National Rural Water Association and Missouri Rural Water Association will not be subjected to the expected costs associated with complying or failing to comply with EPA's modified regulatory requirements under the Cybersecurity Rule.

39. While PWSD #2 will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA's Cybersecurity Guidance as potential "significant deficiencies" if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 10th day of May 2023.

A handwritten signature in blue ink that reads "Sharon A. Cornelius". The signature is written in a cursive style and is positioned above a horizontal line.

Sharon A Cornelius

Manager

Public Water Supply District #2 of Andrew County

Exhibit I

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF JOHN R. DUNN

I, John R. Dunn, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.
2. I am the Director of the City of Ames, Iowa Water and Pollution Control Department (“City of Ames” or the “City”) and have served in this role since 2007. I previously held the position of Assistant Director for eight years, staff environmental engineer for three years, and wastewater laboratory analyst for a different public utility for six years.

3. I have a Bachelor of Science degree in Chemical Engineering from Iowa State University, which I received in 1992, and a Master of Business Administration from Iowa State University, which I received in 2004. I am also a registered professional engineer in the State of Iowa in the branch of environmental engineering.

4. In my capacity as Director, I am required to oversee all activities related to water collection and treatment for the City of Ames, including those involving compliance with the Safe Drinking Water Act (“SDWA”) as well as state law. For its service area, the City of Ames has responsibility over the collection of groundwater through a network of wells, treatment of that water to make it suitable for human consumption, and distribution of the treated water to its customers through a distribution system comprising almost 250 miles of water mains. The City serves more than 18,000 homes and businesses, including the Iowa State University campus and the United States Department of Agriculture’s National Centers for Animal Health. The City’s utility operations, including new capital improvements to meet changing water demands and regulatory standards, are funded through revenue from its customers.

5. As part of my responsibilities, I am involved in the City of Ames’s decision-making about how to prepare for state-conducted sanitary surveys and our cybersecurity practices. I am also actively involved in other aspects of the City of

Ames's operations, including budgeting and rate setting, capital planning, and coordination with local policy makers. I follow new developments in the City of Ames's compliance obligations, including those issued by the U.S. Environmental Protection Agency ("EPA" or the "Agency") and the State of Iowa. I provide feedback to these entities, including through the American Water Works Association ("AWWA"), to ensure that the City's concerns are raised for consideration and its interests protected.

6. The City of Ames is a member of AWWA and the City of Ames relies on AWWA to advocate for its interests, including in EPA rulemakings and in cases such as this one. I am also personally an individual member of AWWA. I serve as Iowa's representative on the AWWA Board of Directors, and I am the Management Committee Chair for the Iowa Section-AWWA

7. I am familiar with EPA's March 3, 2023, memorandum entitled "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process" ("Cybersecurity Rule"), available at <https://tinyurl.com/mswu6xch>, which revises EPA's interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems ("PWSs") to now require evaluation of a system's cybersecurity measures as part of a sanitary survey. The Cybersecurity Rule, as I understand it, requires that if a state identifies a cybersecurity-related "significant deficiency" (i.e., a defect, malfunction, failure, or similar deficiency that has caused

or could cause introduction of contamination to drinking water distributed to customers) as part of a sanitary survey, it must record the significant deficiency, in a publicly available record, and requires the PWS to address the deficiency.

8. I am also familiar with the guidance document accompanying the Cybersecurity Rule, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance” or “Guidance”), available at <https://tinyurl.com/bdfhfrdj>. The Cybersecurity Guidance, at section 7.0, lists sixteen potential cybersecurity-related significant deficiencies and provides, at Appendix A, a checklist of thirty-six cybersecurity controls addressing cybersecurity considerations such as account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

9. I am also aware that the Cybersecurity Guidance provides that the lack (or inadequacy) of a particular cybersecurity control contained in the Appendix A checklist is a potential significant deficiency. These control measures include, as examples, the PWS maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT

and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers.

10. I am aware that the Cybersecurity Rule and Guidance were issued and made immediately effective without EPA providing interested parties, like the City of Ames, the customary notice-and-comment period.

11. The State of Iowa conducts sanitary surveys on a triennial basis. Since it operates a PWS, the City of Ames is already subject to periodic sanitary surveys conducted by the State of Iowa and will continue to be subject to future sanitary surveys, with the next sanitary survey scheduled for Fall 2023.

12. In advance of a sanitary survey, the City of Ames takes steps to avoid a finding of significant deficiency. Not only can significant deficiencies be costly to resolve, but the State's deficiency findings are generally made publicly available, which can undermine the confidence of the City's customers in their water system. In other words, a finding of significant deficiency can often result in both financial and reputational harms.

13. As I understand it, EPA issued the Cybersecurity Rule and Guidance as immediately effective, meaning that its requirements apply to the State of Iowa's sanitary surveys now and that the City of Ames's cybersecurity practices will be evaluated by the State during its next annual sanitary survey in the fall of 2023.

14. To the best of my knowledge, the State of Iowa has not previously conducted cybersecurity evaluations as part of its sanitary surveys of the City of Ames. The City has therefore not previously faced the possibility of a finding of significant deficiency stemming from its cybersecurity practices and systems.

15. The City of Ames is directly subject to Iowa’s implementation of EPA’s requirements under the Cybersecurity Rule and Guidance. The Cybersecurity Rule provides that states “must” “evaluate the adequacy of the cybersecurity of [the] operational technology [used by a PWS] for producing and distributing safe drinking water.” Cybersecurity Rule, at 2–3. And the Rule further requires that “[i]f state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency.” *Id.* My understanding is that as-a PWS, the Cybersecurity Rule and Guidance imposes compliance obligations on the City of Ames.

16. The City of Ames presently has controls in place to address the cybersecurity needs for its water system, and has conducted internal cybersecurity audits to determine areas of improvement. But the City’s controls are tailored to its particular operational needs, and thus do not perfectly align with the six-page list of controls provided in the Cybersecurity Guidance, including the list of 16 “potential significant deficiencies” included by EPA.

17. Given that the Cybersecurity Rule uses mandatory language, I do not believe that the City of Ames has any option other than to implement the suite of cybersecurity controls listed in the Cybersecurity Guidance. Otherwise, the City of Ames risks a finding of significant deficiency during our next sanitary survey. We are therefore already undertaking discussions and expending time on how to best implement EPA's requirements and how to adjust our budget and operations to do so.

18. Some of the cybersecurity controls listed in EPA's Cybersecurity Guidance will take meaningful lead time to implement, which is particularly true for water systems like ours that are subject to municipal budgetary processes. It often takes several budgetary cycles and ample advance planning to have particular budget proposals approved. The City, thus, does not have the leeway to wait and see whether the State of Iowa adopts the entire Cybersecurity Guidance checklist before taking steps to implement those items that could form the basis of a finding of significant deficiency. Instead, the City will need to begin expending resources to both familiarize itself with the requirements of EPA's Cybersecurity Rule and Guidance and implement EPA's suite of cybersecurity controls in order to avoid a finding of significant deficiency.

19. The City of Ames has already expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and

Guidance, and to develop a plan to implement the requirements contained therein. The City will likely need to convene an internal working group including those involved with water system operations, IT, purchasing, and legal—all at the expense of labor hours.

20. Based on a preliminary examination of our existing cybersecurity controls as compared to those listed in the Cybersecurity Guidance checklist, there are at least a few controls that the City of Ames does not presently have in place. The City, as an example, does not maintain an updated inventory of all OT and IT assets, nor updated documentation of the configurations and network topologies of OT and IT assets. Thus, we would likely need to contract with an outside supervisory control and data acquisition (“SCADA”) specialist to assess our OT and IT assets and compile documentations regarding configurations and network topologies. Additionally, the City does not actively integrate cybersecurity considerations as part of its evaluation processes for procurement of OT assets and services. Thus, we would likely need to expend time and resources reviewing our current procurement contracts, which often use standard form language that has been developed and approved over time, and may even need to attempt to renegotiate the terms of existing procurement contracts. These actions would also require time and input from the City’s legal department, and potentially outside counsel given the complexities of cybersecurity. For example, we own and operate a municipal electric

utility. Having differing cyber obligations between the two utilities would impose a significant burden on our IT staff simply to track and continuously confirm ongoing conformance with the EPA checklist.

21. There may be other differences in the controls the City has in place and those listed in the Guidance, and a more intensive audit of the City's cybersecurity systems to determine conformance or nonconformance will likely incur additional internal labor and/or contractor costs.

22. Because EPA's Cybersecurity Rule and Guidance instruct states to look for particular cybersecurity controls, including those highlighted above, and identifies many of those controls as bases for potential "significant deficiencies," the City of Ames will need to make capital investments to change existing cybersecurity controls and implement new ones in anticipation of the City's next sanitary survey to avoid any potential finding of significant deficiency. The City of Ames also has a series of cybersecurity projects that are currently authorized in our budget. Those must now be placed on hold to allow time for us to verify that those improvements are consistent with the checklist, thus delaying the very benefits that are the ultimate intent of the rule.

23. The City of Ames estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to increase by at least \$20,000 per year

to fund new security systems and programs, training and other related expenses. For a customer-funded PWS whose rates are subject to municipal approval, such an increase in cost would be significant. Additional costs, like those stemming from the Cybersecurity Rule, are often passed on to our customers in the form of higher rates. Because the Cybersecurity Rule was made immediately effective, however, the City of Ames did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans. The resulting uncertainty regarding rate planning and cost recovery—and the need to communicate any incremental increases in rates to customers—will create additional implementation challenges.

24. The imposition of this immediate, mandatory obligation means that other critical infrastructure expenditures will need to be delayed. The City of Ames does not carry any undesignated contingency funds in its capital budget. The only options are either to increase rates or delay other critical infrastructure investments. This is coming at a time when both our operating and capital costs are rising dramatically and our ability to maintain adequate funding to cover essential expenses is severely stressed.

25. If Iowa requires additional, more restrictive, or differing cybersecurity controls, as compared to EPA's Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the

lead time necessary to implement some cybersecurity measures, the City of Ames will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

26. In preparation for sanitary surveys, the City of Ames spends time and money to assemble the documents and records that state inspectors will review as part of the survey. For future sanitary surveys under the Cybersecurity Rule, the City of Ames will likely incur significant monetary and internal labor costs to assemble an often-complex set of documents and records in anticipation of a sanitary survey in order to document its compliance with the applicable cybersecurity review program and to allow the State of Iowa to authenticate the City's compliance. Because the City has not previously needed to make such preparations prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would need to be created from scratch, requiring the City to incur additional monetary and internal labor costs.

27. Currently the City does not employ a process control specialist at the water utility. All of the preparations will need to come from an outside vendor. This would also require that the City of Ames have that outside vendor present during our sanitary surveys to be able to answer questions about the operation and configuration of our cybersecurity measures.

28. Importantly, the City of Ames does not presently have on its payroll a dedicated cybersecurity professional with the necessary qualifications and experience to manage and review the type of cybersecurity operations specific to PWSs and contemplated under EPA's Cybersecurity Rule. The Water and Pollution Control Department's cybersecurity operations are presently handled by the City's IT department, meaning that the Water and Pollution Control Department does not have specialized expertise related to the cybersecurity needs of PWSs. Thus, in order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the requirements of EPA's Cybersecurity Rule, the City will likely need to expend money to either hire a dedicated cybersecurity professional or contract with a third party to perform similar cybersecurity services. We estimate that hiring a cybersecurity professional will cost upwards of \$140,000 per year. And the increased demand for such professionals across PWSs as a result of the Cybersecurity Rule will make it all the more difficult to hire or contract with qualified cybersecurity professionals.

29. The Cybersecurity Rule lays out three distinct approaches that states should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the State of Iowa (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative state programs to assess cybersecurity gaps (which must be at least as

stringent as a sanitary survey), any of these approaches will require the City of Ames to expend time, money, and resources in order to undertake the assessment or prepare in advance of a sanitary survey or alternative state program assessment. The City will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

30. I anticipate that the City of Ames, and ultimately its customers, will face the costs described herein unless the Cybersecurity Rule is found unlawful and set aside.

31. Additionally, while the Cybersecurity Rule purports to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, I have grave concerns with an approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of the City's control.

32. Under EPA regulations, a community water system, like the City of Ames, must disclose in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if such deficiency is not corrected to the state's satisfaction prior to the next sanitary survey. In addition, reports from sanitary surveys are generally submitted to City government officials, such as the Mayor's office, and those records are generally considered public documents under Iowa law, namely the Iowa Open Records Law. Because the Cybersecurity Rule

categorizes cybersecurity gaps as potential significant deficiencies, I am concerned that any such gaps identified as part of a sanitary survey would likely be made public, whether by way of consumer confidence reports or as records made available under open records laws. Not only would public disclosure of cybersecurity-related significant deficiencies undermine customer trust in their water system—even if the system’s cybersecurity measures are particularly robust despite not encompassing every cybersecurity measure in EPA’s six-page checklist—but also make that system vulnerable to targeting by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

33. Relatedly, as the Director of the City of Ames Water & Pollution Control Department, I have concerns about providing copies of cybersecurity documents, such as OT and IT inventories and configurations, to state officials. The City’s existing cybersecurity procedures require maintaining secure control over such documents and limiting outside access. This procedure is designed to limit the availability of information that could be used by nefarious actors to discover and target potential weaknesses in the City’s systems. This control is weakened, however, if copies of sensitive cybersecurity documents are given to outside entities, including regulators, over which the City has no control or assurance of security. In other words, some of EPA’s cybersecurity controls are likely to directly conflict with

the City's existing cybersecurity controls, namely control of cybersecurity-related documents.

34. The City of Ames was subject to the requirement to complete an updated AWIA Risk and Resilience Assessment ("RRA") that included cybersecurity. The outcome of that assessment is a set of already planned and funded projects. One of the explicitly identified countermeasures was to keep the contents of that RRA confidential. Releasing these documents would therefore conflict with our existing AWIA Emergency Response Plan.

35. Even if Iowa is permitted to make deficiencies confidential, there is still the acute risk that a hacker or similar bad actor will target the state's database to obtain information regarding potential cybersecurity vulnerabilities across the state's jurisdiction. By centralizing potentially harmful information about a system's vulnerability, I contend that the Cybersecurity Rule places the City of Ames and all other Iowa water utilities at greater risk of a cyberattack.

36. In my capacity as Director of Water and Pollution Control for the City of Ames, I have discussed the Cybersecurity Rule with other PWSs, who have shared similar concerns with the rule and associated guidance.

37. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided issuing the rule pursuant to formal notice and comment under the Administrative Procedure Act ("APA"). If the Cybersecurity Rule and Guidance had

been subject to notice and comment pursuant to the APA, I would have recommended that the City of Ames, either independently or through the AWWA, raise its concerns including those described herein, for EPA's consideration. The City has previously done so for a variety of EPA SDWA regulations, including the Agency's revisions to its lead and copper rule, as well as its national primary drinking water regulations for per- and polyfluoroalkyl substances (commonly known as "PFAS").

38. As a regulated entity under the SDWA, the City of Ames has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient. I believe that the City has been deprived of a fair and transparent regulatory process to protect those interests and provide EPA with industry insight and experience.

39. Relatedly, if EPA had proposed the Cybersecurity Rule through the normal APA procedures, the City of Ames would have had more advance notice of the likely requirements in the rule, which would have assisted the City of Ames in budgeting and planning accordingly. Most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded the City additional time to prepare for the implementation of the requirements.

40. I am generally familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa (“Petitioners”), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule.

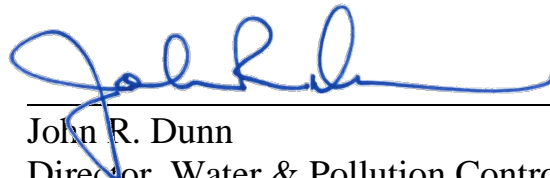
41. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA’s compliance with notice-and-comment procedures required by the APA, the City of Ames, a member of AWWA, will not be subjected to the expected costs and cybersecurity risks associated with complying or failing to comply with EPA’s modified regulatory requirements under the Cybersecurity Rule.

42. The City of Ames will continue to implement those cybersecurity measures that it identifies as providing meaningful improvements to the City’s cybersecurity posture. But should the Cybersecurity Rule be held unlawful and be set aside, I would not recommend that the City undertake any measures that expend our ratepayers’ funds without a tangible benefit.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 9th day of May 2023.



John R. Dunn
Director, Water & Pollution Control
Department
City of Ames, Iowa

Exhibit J

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF JACKIE WILLIAM HINCHEY, JR,

I, Jackie William Hinchey, Jr, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.

2. I am the Manager of the City of Clinton Water and Sewer Department. I have served in this role since 2019. Previously, I held the position of the water and sewer superintendent of the City of Leslie Water and Sewer. I have a Wastewater 3 License and a Water Distribution 4 License. I also have a plumbing inspector license.

3. Clinton Water and Sewer Department (“Clinton Water”) is a water utility headquartered in Clinton, Arkansas. Clinton Water serves a population of 7,578 customers

inside and outside the city of Clinton. We also provide water to the Bee Branch Water Association and Van Buren County Association.

4. Clinton Water is a member of the National Rural Water Association (“NRWA”) through the Arkansas Rural Water Association. Clinton Water relies on NRWA to advocate for its interests, including before federal agencies like the U.S. Environmental Protection Agency (“EPA”).

5. In my capacity as Manager, I am required to oversee all activities related to drinking water distribution for Clinton Water’s service area, including those involving compliance with the federal Safe Drinking Water Act (“SDWA”) as well as state law. As a result, I follow new developments in the law, including changes issued by either the U.S. Environmental Protection Agency (“EPA”) or the State of Arkansas. I also provide feedback to the federal and state government, including through NRWA to ensure that Clinton Water’s concerns are raised and its interests are protected.

6. As part of my responsibilities, I am involved in Clinton Water’s decision-making about how to prepare for sanitary surveys and our cybersecurity practices. As Manager, I am also actively involved in other aspects of Clinton Water’s operations, including financial, utility management, field operations, and construction.

7. I am familiar with EPA’s March 3, 2023, memorandum entitled “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process” (“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises EPA’s interpretations of its

SDWA regulations regarding state-conducted sanitary surveys of public water systems (“PWSs”) to include evaluations of a system’s cybersecurity measures as part of a survey. I know that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related “significant deficiency”—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

8. I am also familiar with EPA guidance accompanying the Cybersecurity Rule, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance”), available at <https://tinyurl.com/bdfhfrdj>. I am aware that Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing things like account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

9. I also know that section 7.0 of the Cybersecurity Guidance tells utilities that if they are missing a particular cybersecurity control contained in the checklist, it is a potential significant deficiency. These control measures include, as examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network

components) across its OT and IT networks, and including cybersecurity considerations in evaluating vendors and/or service providers.

10. I understand that the State of Arkansas, through the Arkansas Department of Health, administers the SDWA within Arkansas and as part of those responsibilities conducts a sanitary survey of our PWS every 3 years. As a PWS, Clinton Water is already subject to periodic sanitary surveys conducted by the Arkansas Department of Health and will continue to be subject to future sanitary surveys.

11. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements apply to Clinton Water now and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

12. Before the Arkansas Department of Health conducts the next sanitary survey, Clinton Water takes steps to avoid a finding of a significant deficiency. We seek to avoid any significant deficiencies because they can be costly to correct and they can undermine the confidence of our customers in our practices because the findings are made public. A finding of a significant deficiency therefore causes both financial, community loss of confidence, and reputational harm to Clinton Water.

13. As far as I am aware, the Arkansas Department of Health has not previously conducted cybersecurity evaluations as part of its sanitary surveys of Clinton Water because such evaluations have not been required under EPA's regulations. As a result,

Clinton Water has not previously faced the risk of a “significant deficiency” as a result of any of its cybersecurity practices.

14. Clinton Water is directly subject to Arkansas’s implementation of the new cybersecurity evaluation requirements under EPA’s Cybersecurity Rule and Guidance. Because the Cybersecurity Rule says that “states must do the following to comply with the requirement to conduct a ‘sanitary survey’” and “if the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency” we understand that the Cybersecurity Rule and Guidance applies directly to us.

15. Clinton Water uses an industrial control system (“ICS”) or other operational technology as part of the equipment or operation of some required components of the sanitary surveys.

16. While Clinton Water does have measures in place to address cybersecurity concerns, those measures do not align with all of the specific requirements outlined in EPA’s Cybersecurity Guidance. Clinton Water’s current cybersecurity measures are instead tailored to its specific operational needs.

17. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA as potential significant deficiencies in section 7.0 of the Guidance (“Cybersecurity Checklist”). We are already trying our best

to implement these requirements and deciding how to adjust our budget and operations to do so.

18. Some of the items listed in EPA's Cybersecurity Checklist of "significant deficiencies" will take meaningful lead time to implement, particularly given how we budget. As a result, Clinton Water cannot afford to wait and see whether Arkansas adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential significant deficiencies. Instead, Clinton Water must begin spending money and time now to become familiar with the new requirements and act to avoid EPA's list of significant deficiencies.

19. Clinton Water has already spent time, money, and energy to review the new requirements contained in EPA's Cybersecurity Rule and Guidance, and to develop a plan to implement the EPA's new requirements. For example, Clinton Water has spent time researching the Cybersecurity Rule and Guidance and has determined that Clinton Water will be required to hire outside cybersecurity contractors to assess and determine what actions will be needed to protect all of our computer software systems and SCADA systems. All expenses for the cybersecurity services will require additional revenues to be budgeted and will require customer rate increases to raise revenue in order to cover the increased expenses for the new cybersecurity contract services. Arkansas has over 650 community water systems in the state that will be directly affected by the New Cybersecurity Rule that will require outside cybersecurity contractors to assist each

community water systems as the water utilities do not have staff trained to identify and install cybersecurity protection.

20. Based on preliminary look at our existing cybersecurity controls as compared to those listed in the Cybersecurity Checklist, there are at least a few controls that Clinton Water does not presently have in place and/or that will pose operational challenges on Clinton Water.

21. Because EPA's Cybersecurity Rule and Guidance tell states to look for particular cybersecurity controls, including those highlighted above, and identifies those controls as potential "significant deficiencies," *see* Cybersecurity Guidance, at 11–14, Clinton Water will need to make capital investments to enhance existing cybersecurity controls and implement new ones in anticipation of Clinton Water's next sanitary survey to avoid any potential finding of significant deficiency.

22. Clinton Water estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be increased.

23. Because the Cybersecurity Rule was made immediately effective, Clinton Water did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for Clinton Water.

24. In many instances, additional costs like those stemming from the Cybersecurity Rule are passed on to our customers in the form of higher rates. Because the Cybersecurity Rule was made immediately effective, Clinton Water did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, and we were unable to make smaller incremental increases to our rates or otherwise communicate the changes to our customers, which harms our relationship with those customers.

25. If Arkansas requires additional, more restrictive, or different cybersecurity controls as a result of EPA's Cybersecurity Rule and Guidance, we will likely need to incur additional internal labor, contractor, and/or capital costs. And given the lead time necessary to implement some cybersecurity measures, Clinton Water will likely need to act early to assess and update its cybersecurity controls and systems prior to its next sanitary survey, rather than wait for the state to implement these different requirements.

26. In order to prepare for sanitary surveys, Clinton Water spends time and money assembling documents that will be reviewed as part of the survey. For future sanitary surveys under the Cybersecurity Rule, Clinton Water will incur additional monetary and internal labor costs to assemble the documents and records to demonstrate that we comply with the new Cybersecurity Rule requirements. Because Clinton Water has not previously needed to do this work prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would need to be

created from scratch, requiring Clinton Water to incur additional monetary and internal labor costs.

27. Clinton Water does not presently have on its payroll a cybersecurity expert to manage and review the type of cybersecurity operations in EPA's rule. Thus, in order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, Clinton Water will likely need to expend money to either hire a cybersecurity expert or hire a contractor to do similar work. The demand for cybersecurity experts will make it difficult for Clinton Water to hire one without changes to its budget. In the meantime, the burden of evaluating EPA's Cybersecurity Rule will fall on Clinton Water's existing IT staff and will therefore limit our staff's ability to focus on our other IT needs.

28. The Cybersecurity Rule lays out three options for States in including cybersecurity in PWS sanitary surveys. Regardless of whether Arkansas (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require Clinton Water to expend time, money, and resources in order to assess or prepare in advance of a sanitary survey or alternative State program assessment. Clinton Water will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

29. Clinton Water, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

30. Additionally, while the Cybersecurity Rule proposes to allow States the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, Clinton Water has concerns with an approach that puts information about its potential cybersecurity gaps in a centralized database outside of Clinton Water's control.

31. Under EPA regulations, a community water system, like Clinton Water must list in its annual "consumer confidence report" a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state's satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule states that cybersecurity gaps are potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our system vulnerable to hackers or similar bad actors who can exploit potential cybersecurity gaps.

32. Even if Arkansas can confidentially protect significant deficiencies or other cybersecurity information, hackers or similar bad actors may still target the state's database to get information regarding potential cybersecurity vulnerabilities across the state. By centralizing potentially harmful information about a system's vulnerability, the Cybersecurity Rule therefore places Clinton Water at greater risk of a cyberattack.

33. Clinton Water has talked about the Cybersecurity Rule with other PWSs, who have shared similar concerns with the rule and associated guidance.

34. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act (“APA”) that would have provided Clinton Water with an opportunity to raise these concerns with the requirements through the notice and comment. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant to the APA, Clinton Water either independently or through NRWA would have raised its concerns including those described above, for EPA’s consideration.

35. As a water utility subject to the SDWA, Clinton Water has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect its interests and provide EPA with industry insight and experience.

36. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, Clinton Water would have had more advanced notice of the likely requirements in the rule, which would have assisted Clinton Water in budgeting and planning accordingly. In addition, because most regulations issued under APA procedures allow some time before going into effect, Clinton Water would have had additional time to prepare for the implementation of the requirements.

37. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA’s compliance with notice and comment procedures required by the APA,

Clinton Water, a member of NRWA through the Arkansas Rural Water Association, will not face the expected costs associated with complying or failing to comply with EPA’s modified regulatory requirements under the Cybersecurity Rule.

38. While Clinton Water will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA’s Cybersecurity Guidance as potential “significant deficiencies” if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 12th day of May 2023.

A handwritten signature in blue ink that reads "Jackie William Henchey Jr." The signature is written in a cursive style and is positioned above a horizontal line.

Exhibit K

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF RANDAL PLEIMA

I, Randal Pleima, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.

2. I am General Manager of the Mahaska Rural Water System, Inc (MRWS). I have served in this role since 1985. Previously, I held the position of Water treatment and Distribution operator with MRWS for 2 years

3. I have 1 year of trade schooling post high school with a degree in electrical. I currently hold in the State of Iowa a Grade IV Water Distribution License, a Grade III Water Treatment License, and a Grade I Wastewater License. I

have served on the Iowa Rural Water Association Board of Directors for over 25 years and have served as President for 13 years and I'm currently Vice-President on the Board. Serving Rural Iowa and its Rural Communities has been my life long passion and job

4. MRWS is headquartered in Oskaloosa, Iowa. MRWS serves its 4023 individual customers water and 725 wastewater customers in Mahaska County and small parts of Marion, Wapello, and Monroe Counties.

MRWS is a member of NRWA.

5. In my capacity as General Manager, I am required to oversee all activities related to drinking water distribution for MRWS service area including those involving compliance with the federal Safe Drinking Water Act ("SDWA") as well as state law. As a result, I follow new developments in MRWS compliance obligations issued by either the U.S. Environmental Protection Agency ("EPA") or the State of Iowa. I also provide feedback to these entities, including through NRWA, to ensure that MRWS concerns are raised and its interests are protected.

6. As part of my responsibilities, I am involved in MRWS decision-making about how to prepare for sanitary surveys and our cybersecurity practices. As General Manager, I am also actively involved in other aspects of MRWS operations, including financial, board management, field operations, and construction.

7. I am familiar with EPA’s March 3, 2023, memorandum entitled “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process” (“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises EPA’s interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems (“PWSs”) to include evaluations of a system’s cybersecurity measures as part of a survey. I am aware that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related “significant deficiency”—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

8. I am also familiar with the EPA guidance document accompanying the Cybersecurity Rule, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance”), available at <https://tinyurl.com/bdfhfrdj>. I am aware that Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing general areas of concern including account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

9. I am also aware that section 7.0 of the Cybersecurity Guidance provides that the lack of or inadequacy of a particular cybersecurity control contained in the checklist is a potential significant deficiency. These control measures include, as examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers.

10. I understand that the Iowa DNR administers the SDWA within its borders and as part of those responsibilities conducts a sanitary survey of PWS every 3 years. As a PWS, MRWS is already subject to periodic sanitary surveys conducted by Iowa DNR and will continue to be subject to future sanitary surveys.

11. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements apply to MRWS now and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

12. MRWS takes steps in advance of the sanitary surveys to avoid a finding that there is a significant deficiency in any of its practices. We seek to avoid any significant deficiencies because they can be costly to correct and they can undermine

the confidence of our customers in our practices because the findings are made public. A finding of a significant deficiency therefore causes both financial and reputational harm to MRWS and to all of our water and sewer customers who rely on us to provide safe and dependable service 24 hours a day.

13. As far as I am aware, Iowa DNR has not previously conducted cybersecurity evaluations as part of its sanitary surveys of MRWS because such evaluations have not been required under EPA's regulations. As a result, MRWS has not previously faced the risk of a "significant deficiency" as a result of any of its cybersecurity practices.

14. MRWS is directly subject to Iowa's DNR implementation of the new cybersecurity evaluation requirements under EPA's Cybersecurity Rule and Guidance. Because the Cybersecurity Rule states that "states must do the following to comply with the requirement to conduct a 'sanitary survey'" and Iowa DNR determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency" we understand that the Cybersecurity Rule and Guidance applies directly to us.

15. While MRWS does have measures in place to address cybersecurity concerns, those measures do not align with all of the specific requirements outlined

in EPA's Cybersecurity Guidance. MRWS's current cybersecurity measures are instead tailored to its specific operational needs.

16. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA as potential significant deficiencies in section 7.0 of the Guidance ("Cybersecurity Checklist"). We are already undertaking discussions on how to best implement these requirements and how to adjust our budget and operations to do so.

17. Some of the items listed in EPA's Cybersecurity Checklist of "significant deficiencies" will take meaningful lead time to implement, particularly given the nature of our budgeting. As a result, MRWS cannot afford to wait and see whether the State of Iowa adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential significant deficiencies. Instead, MRWS must begin expending resources now to familiarize itself with the new requirements and to implement measures to avoid EPA's list of significant deficiencies.

18. MRWS has already expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and Guidance, and to develop a plan to implement the requirements contained therein. *Beginning In January 2023, MRWS has enter into to a contract with a local firm Access*

Systems located in Des Moines, Iowa to help and to do 24 hour monitoring of our system and computer hardwares. To date MRWS has expended over \$26,000.00 to upgrade to a main computer server and additional backup capabilities, new login procedures, battery backups, and better security to our current SCADA system. MWRS has signed a 3 year deal for continuous monitoring for an additional cast of \$1,086.00 per month

19. Based on a preliminary examination of our existing cybersecurity controls as compared to those listed in the Cybersecurity Checklist, there are at least a few controls that MRWS does not presently have in place.

20. Because EPA's Cybersecurity Rule and Guidance instruct states to look for particular cybersecurity controls, including those highlighted above, and identifies those controls as potential "significant deficiencies," *see* Cybersecurity Guidance, at 11–14, MRWS will need to make capital investments to enhance existing cybersecurity controls and implement new ones in anticipation of [organization]'s next sanitary survey to avoid any potential finding of significant deficiency.

21. MRWS estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be increased drastically after MRWS has spent its 2023 budget allowances.

22. Because the Cybersecurity Rule was made immediately effective, MRWS did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for MRWS.

23. In many instances, additional costs like those stemming from the Cybersecurity Rule are passed on to our customers in the form of higher rates. Because the Cybersecurity Rule was made immediately effective, MRWS did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, we were unable to make smaller incremental increases to our rates or otherwise communicate the changes to our customers, which harms our relationship with those customers.

24. If Iowa DNR requires additional, more restrictive, or differing cybersecurity controls as a result of EPA's Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the lead time necessary to implement some cybersecurity measures, MRWS will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

25. In order to prepare for sanitary surveys, MRWS spends time and money assembling documents that will be reviewed as part of the survey.

26. For future sanitary surveys under the Cybersecurity Rule, MRWS will likely incur significant additional monetary and internal labor costs to assemble a complex set of documents and records to demonstrate its compliance with the applicable cybersecurity review program and to allow the State of Colorado to authenticate MRWS's compliance. Because MRWS has not previously needed to make such preparations prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would need to be created from scratch, requiring MRWS to incur additional monetary and internal labor costs.

27. MRWS, which operates with Iowa DNR administrative and operations personnel, does not presently have on its payroll a dedicated cybersecurity professional with the requisite qualifications and experience to manage and review the type of cybersecurity operations contemplated under EPA's rule. Thus, in order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, MRWS will likely need to expend money to either hire a dedicated cybersecurity professional or contract with a third party to perform similar cybersecurity services. The demand for qualified personnel capable of performing the work required by the Cybersecurity Rule will make it difficult for

[organization] to hire a dedicated employee for this role without changes to its budget.

28. The Cybersecurity Rule lays out three distinct approaches that States should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the State of Iowa (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require [organization] to expend time, money, and resources in order to undertake the assessment or prepare in advance of a sanitary survey or alternative State program assessment. MRWS will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

29. MRWS, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

30. Additionally, while the Cybersecurity Rule proposes to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, MRWS has concerns with an approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of MRWS's control.

31. Under EPA regulations, a community water system, like MRWS, must disclose in its annual “consumer confidence report” a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state’s satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule categorizes cybersecurity gaps as potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our system vulnerable to targeting by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

32. Even if Iowa is permitted to make deficiencies or other information that it collects related to our cybersecurity practices confidential, there is still the acute risk that a hacker or similar bad actor will target the state’s database to obtain information regarding potential cybersecurity vulnerabilities across the state’s jurisdiction. By centralizing potentially harmful information about a system’s vulnerability, the Cybersecurity Rule therefore places [organization] at greater risk of a cyberattack.

33. MRWS has discussed the Cybersecurity Rule with other PWSs, who have shared similar concerns with the rule and associated guidance.

34. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act (“APA”) that would have provided MRWS with an opportunity to raise these concerns with the

requirements through the APA's public notice and comment provisions. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant to the APA, MRWS, either independently or through the NRWA, would have raised its concerns including those described herein, for EPA's consideration.

35. As a regulated entity under the SDWA, MRWS has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect its interests and provide EPA with industry insight and experience.

36. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, MRWS would have had more advanced notice of the likely requirements in the rule, which would have assisted MRWS in budgeting and planning accordingly. In addition, most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded [organization] additional time to prepare for the implementation of the requirements.

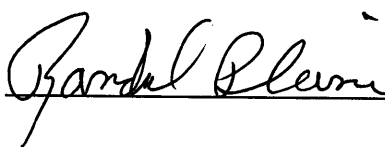
37. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA's compliance with notice and comment procedures required by the APA, MRWS, a member of NRWA, will not be subjected to the expected costs associated with complying or failing to comply with EPA's modified regulatory requirements under the Cybersecurity Rule.

38. While MRWS will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA’s Cybersecurity Guidance as potential “significant deficiencies” if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 7th day of May 2023.

A handwritten signature in black ink, appearing to read "Randal Pleima", is written over a solid horizontal line.

Randal Pleima

General Manager

Mahaska Rural Water System, Inc.

Exhibit L

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

STATE OF MISSOURI, STATE OF
ARKANSAS, and STATE OF IOWA,

Petitioners,

v.

MICHAEL REGAN, Administrator,
U.S. Environmental Protection
Agency, UNITED STATES
ENVIRONMENTAL PROTECTION
AGENCY, and RADHIKA FOX,
Assistant Administrator, U.S.
Environmental Protection Agency,

Respondents

No. 23-1787

DECLARATION OF SHILO WILLIAMS

I, Shilo Williams, swear or affirm under penalty of perjury, the following:

1. I base this Declaration upon my first-hand knowledge of the matters described herein. I am over the age of 21 and am competent to make this Declaration.
2. I am the Environmental Superintendent for the City and Borough of Sitka (CBS). I have served in this role since 2015.
3. I hold an Associates of Applied Science with an Emphasis on Water Quality Management.
4. The CBS is located on Baranof island in southeast Alaska and has a population of approximately 8,500.

5. The CBS is a member of is a member of AWWA and relies on AWWA to help represent its interests, including in EPA rulemakings and in cases such as this one.

6. In my capacity as Environmental Superintendent, I am required to oversee all activities related to drinking water distribution for the CBS service area including those involving compliance with the federal Safe Drinking Water Act (“SDWA”) as well as state law. As a result, I follow new developments in CBS compliance obligations issued by either the U.S. Environmental Protection Agency (“EPA”) or the State of Alaska. I also provide feedback to these entities, including through AWWA, to ensure that CBS concerns are raised and its interests are protected.

7. As part of my responsibilities, I am involved in CBS’s decision-making about how to prepare for sanitary surveys and our cybersecurity practices. As Environmental Superintendent, I am also actively involved in other aspects of CBS operations, including financial, field operations, and construction activities.

8. I am familiar with EPA’s March 3, 2023, memorandum entitled “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternative Process” (“Cybersecurity Rule”), available at <https://tinyurl.com/mswu6xch>, which revises EPA’s interpretations of its SDWA regulations regarding state-conducted sanitary surveys of public water systems (“PWSs”) to include evaluations of a system’s

cybersecurity measures as part of a survey. I am aware that the Cybersecurity Rule requires that if a state identifies a cybersecurity-related “significant deficiency”—i.e., a defect, malfunction, failure, or similar deficiency that has caused or could cause introduction of contamination to drinking water distributed to customers—as part of a sanitary survey, it must require the PWS to address the significant deficiency.

9. I am also familiar with the EPA guidance document accompanying the Cybersecurity Rule, entitled “Evaluating Cybersecurity During Public Water System Sanitary Surveys” (“Cybersecurity Guidance”), available at <https://tinyurl.com/bdfhfrdj>. I am aware that Cybersecurity Guidance, at Appendix A, provides a checklist of thirty-six cybersecurity controls addressing general areas of concern including account security, device security, governance and training, vulnerability management, supply chains and third parties, and response and recovery.

10. CBS uses an industrial control system (“ICS”) or other operational technology as part of the equipment or operation of a required component of the sanitary surveys.

11. I am also aware that section 7.0 of the Cybersecurity Guidance provides that the lack of or inadequacy of a particular cybersecurity control contained in the checklist is a potential significant deficiency. These control measures include, as

examples, maintaining an updated inventory of operational technology (“OT”) and information technology (“IT”) assets, maintaining configuration documentation of those assets, maintaining updated documentation describing network topology (i.e., connections between all network components) across its OT and IT networks, and including cybersecurity considerations as part of its evaluative process for vendors and/or service providers.

12. I understand that the State of Alaska Department of Environmental Conservation (ADEC) administers the SDWA within its borders and as part of those responsibilities requires the CBS to conduct a sanitary survey of our PWS every 3 years. As a PWS, CBS is already subject to periodic sanitary surveys conducted by a third party and will continue to be subject to future sanitary surveys. We expect our next sanitary survey to take place in 2024.

13. As I understand it, the Cybersecurity Rule and Guidance were made immediately effective, meaning that their requirements apply to the CBS now and that our cybersecurity practices will be reviewed during the next periodic sanitary survey.

14. The CBS takes steps in advance of the sanitary surveys to avoid a finding that there is a significant deficiency in any of its practices. We seek to avoid any significant deficiencies because they can be costly to correct and they can undermine the confidence of our customers in our practices because the findings are

made public. A finding of a significant deficiency therefore causes both financial and reputational harm to the CBS.

15. As far as I am aware, ADEC has not previously conducted cybersecurity evaluations as part of its sanitary surveys of the CBS because such evaluations have not been required under EPA's regulations. As a result, the CBS has not previously faced the risk of a "significant deficiency" as a result of any of its cybersecurity practices.

16. The CBS is directly subject to ADEC's implementation of the new cybersecurity evaluation requirements under EPA's Cybersecurity Rule and Guidance. Because the Cybersecurity Rule states that "states must do the following to comply with the requirement to conduct a 'sanitary survey'" and "if the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency" we understand that the Cybersecurity Rule and Guidance applies directly to us.

17. While the CBS does have measures in place to address cybersecurity concerns, those measures do not align with all of the specific requirements outlined in EPA's Cybersecurity Guidance. The CBS's current cybersecurity measures are instead tailored to its specific operational needs.

18. The CBS is subject to the AIWA requirements and has completed the required risk and resiliency plan. The new EPA requirements will require the CBS to review and potentially update the risk and resiliency plan. The new EPA requirements will also require the CBS to determine the differences between the AIWA requirements and the new EPA requirements.

19. Because the Cybersecurity Rule uses mandatory language, we do not believe we have any option other than to implement the requirements in the Cybersecurity Guidance, including the thirty-six items listed by EPA as potential significant deficiencies in section 7.0 of the Guidance (“Cybersecurity Checklist”). We are already undertaking discussions on how to best implement these requirements and how to adjust our budget and operations to do so.

20. Some of the items listed in EPA’s Cybersecurity Checklist of “significant deficiencies” will take meaningful lead time to implement, particularly given the nature of our budgeting. As a result, the CBS cannot afford to wait and see whether the State of Alaska adopts this entire Cybersecurity Checklist before beginning to take steps to implement the items identified as potential significant deficiencies. Instead, the CBS must begin expending resources now to familiarize itself with the new requirements and to implement measures to avoid EPA’s list of significant deficiencies.

21. The CBS has already expended time, money, and human capital to review the new requirements contained in EPA's Cybersecurity Rule and Guidance, and to develop a plan to implement the requirements contained therein. The FY24 budget is complete and does not include capital for costs associated with the new EPA Cyber requirements. Budget preparation for the FY25 budget will begin in October 2023. The CBS will need to spend time and money between now and October to determine how much capital will be needed to comply with the new EPA requirements. This could create the need to seek a supplemental appropriation to the FY24 budget which would be faced with public scrutiny.

22. Based on a preliminary examination of our existing cybersecurity controls as compared to those listed in the Cybersecurity Checklist, there are at least a few controls that the CBS does not presently have in place. For example, the lack of written processes, procedures, and training including the overall lack of technical understanding of the new EPA requirements.

23. Because EPA's Cybersecurity Rule and Guidance instruct states to look for particular cybersecurity controls, including those highlighted above, and identifies those controls as potential "significant deficiencies," *see* Cybersecurity Guidance, at 11–14, the CBS will need to make capital investments to enhance existing cybersecurity controls and implement new ones in anticipation of CBS's next sanitary survey to avoid any potential finding of significant deficiency.

24. The CBS estimates that in order to meet the specific requirements provided by the Cybersecurity Rule and Guidance, its cybersecurity and information technology budget will need to be increased.

25. Because the Cybersecurity Rule was made immediately effective, the CBS did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, which will create additional implementation challenges for the CBS.

26. In many instances, additional costs like those stemming from the Cybersecurity Rule are passed on to our customers in the form of higher rates. Because the Cybersecurity Rule was made immediately effective, the CBS did not have any notice or time to prepare for the new requirements or to forecast the associated costs into future budgeting plans, we were unable to make smaller incremental increases to our rates or otherwise communicate the changes to our customers, which harms our relationship with those customers.

27. If ADEC requires additional, more restrictive, or differing cybersecurity controls as a result of EPA's Cybersecurity Rule and Guidance, additional internal labor, contractor, and/or capital costs will likely be required. And given the lead time necessary to implement some cybersecurity measures, the CBS will likely need to be proactive in assessing and updating its cybersecurity controls and systems prior to its next sanitary survey, rather than take a passive approach.

28. In order to prepare for sanitary surveys, the CBS spends time and money assembling documents that will be reviewed as part of the survey.

29. For future sanitary surveys under the Cybersecurity Rule, the CBS will likely incur significant additional monetary and internal labor costs to assemble a complex set of documents and records to demonstrate its compliance with the applicable cybersecurity review program and to allow ADEC to authenticate the CBS's compliance. Because the CBS has not previously needed to make such preparations prior to a sanitary survey, the necessary document and data collection and authentication processes are not presently in place and would need to be created from scratch, requiring the CBS to incur additional monetary and internal labor costs.

30. The CBS Environmental Division, which operates with 11 administrative and operations personnel, does not presently have on its payroll a dedicated cybersecurity professional for our division with the requisite qualifications and experience to manage and review the type of cybersecurity operations contemplated under EPA's rule. Thus, in order to evaluate existing cybersecurity systems and propose, implement, and maintain new and revised cybersecurity controls and systems that align with the new Cybersecurity Rule requirements, the CBS or our division may need to expend money to either hire a dedicated cybersecurity professional or contract with a third party to perform similar

cybersecurity services. The demand for qualified personnel capable of performing the work required by the Cybersecurity Rule will make it difficult for the CBS to hire a dedicated employee for this role without changes to its budget.

31. The Cybersecurity Rule lays out three distinct approaches that States should take to include cybersecurity in PWS sanitary surveys. Regardless of whether the ADEC (1) requires self-assessments or third-party assessments; (2) evaluates cybersecurity practices directly in sanitary surveys; or (3) implements alternative State programs to assess cybersecurity gaps (which must be at least as stringent as a sanitary survey), any of these approaches will require the CBS to expend time, money, and resources in order to undertake the assessment or prepare in advance of a sanitary survey or alternative State program assessment. The CBS will also have to expend additional time and resources to review the EPA technical assistance described in the Cybersecurity Rule and Guidance.

32. The CBS, and ultimately its customers, will face the above-described costs unless the Cybersecurity Rule is found unlawful and set aside.

33. Additionally, while the Cybersecurity Rule proposes to allow states the ability to protect as confidential information about cybersecurity-related significant deficiencies recorded as part of a sanitary survey, The CBS has concerns with an approach that consolidates information about its potential cybersecurity gaps in a centralized database outside of the CBS's control.

34. Under EPA regulations, a community water system, like the CBS, must disclose in its annual “consumer confidence report” a significant deficiency identified during a sanitary survey if the deficiency is not corrected to the state’s satisfaction prior to the next sanitary survey. Because the Cybersecurity Rule categorizes cybersecurity gaps as potential significant deficiencies, such gaps would need to be publicly identified in our annual consumer confidence report, making our system vulnerable to targeting by hackers or similar bad actors seeking to exploit potential cybersecurity gaps.

35. Even if ADEC is permitted to make deficiencies or other information that it collects related to our cybersecurity practices confidential, there is still the acute risk that a hacker or similar bad actor will target the state’s database to obtain information regarding potential cybersecurity vulnerabilities across the state’s jurisdiction. By centralizing potentially harmful information about a system’s vulnerability, the Cybersecurity Rule therefore places the CBS at greater risk of a cyberattack.

36. By treating the Cybersecurity Rule as an interpretative rule, EPA has avoided the procedures in the Administrative Procedure Act (“APA”) that would have provided the CBS with an opportunity to raise these concerns with the requirements through the APA’s public notice and comment provisions. If the Cybersecurity Rule and Guidance had been subject to notice and comment pursuant

to the APA, the CBS, either independently or through the AWWA, would have raised its concerns including those described herein, for EPA's consideration.

37. As a regulated entity under the SDWA, the CBS has a concrete interest in ensuring that regulatory obligations imposed on it are fair, effective, and cost-efficient, and believes that it has been deprived of a fair and transparent regulatory process to protect its interests and provide EPA with industry insight and experience.

38. If EPA had proposed the Cybersecurity Rule through the normal APA procedures, the CBS would have had more advanced notice of the likely requirements in the rule, which would have assisted the CBS in budgeting and planning accordingly. In addition, most regulations issued under APA procedures provide for a period of time before implementation, which would have afforded the CBS additional time to prepare for the implementation of the requirements.

39. I am generally familiar with the petition for review filed by the States of Missouri, Arkansas, and Iowa ("Petitioners"), No. 23-1787 (8th Cir. Apr. 17, 2023), seeking to review and set aside the Cybersecurity Rule.

40. Should the Cybersecurity Rule be held unlawful and set aside, pending, at a minimum, EPA's compliance with notice and comment procedures required by the APA, the CBS, a member of AWWA, will not be subjected to the expected costs associated with complying or failing to comply with EPA's modified regulatory requirements under the Cybersecurity Rule.

41. While the CBS will continue to implement cybersecurity measures, it will not undertake all of the specific items identified by EPA's Cybersecurity Guidance as potential "significant deficiencies" if the Cybersecurity Rule be held unlawful and set aside.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 12th day of May 2023.

Shute Williams