UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF WATER

March 3, 2023

MEMORANDUM

SUBJECT: Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process

FROM: Radhika Fox
Assistant Administrator

TO: State Drinking Water Administrators
Water Division Directors, Regions I-X

Cyber-attacks against critical infrastructure facilities, including public water systems (PWSs), are increasing.[1,2] Past incidents have shown that these attacks have the potential to disable or contaminate the delivery of drinking water to consumers and other essential facilities like hospitals.[3,4,5,6] While some PWSs have taken important steps to improve their cybersecurity, a recent survey[7] and reports of cyber-attacks show that many PWSs have failed to adopt basic cybersecurity best practices and consequently are at high risk of being victimized by a cyber-attack—whether from an individual, criminal collective, or a sophisticated state or state sponsored actor.

The steps described in this memorandum further the mission of the U.S. Environmental Protection Agency (EPA) to work with states to protect clean and safe drinking water. While some states currently oversee cybersecurity at PWSs, EPA clarifies with this memorandum that states must evaluate the cybersecurity of operational technology[8] used by a PWS when conducting PWS sanitary surveys or through other state programs. This memorandum explains various approaches to include cybersecurity in PWS sanitary surveys or other state programs. The goal of sanitary surveys is to ensure that states effectively identify significant deficiencies and that public water systems then correct those significant deficiencies—including cybersecurity-related significant deficiencies—that could impact safe drinking water. EPA is offering significant technical assistance and support to states in this effort as well as to PWSs in helping to close cybersecurity gaps.

---

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
[2] https://www.cisa.gov/uscert/ncas/alerts/aa21-287a
[3] https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206
[4] https://www.wtae.com/article/fbi-investigating-hacking-threats-at-pennsylvania-water-systems/36386504#
[5] https://www.nbcnews.com/tech/security/lye-poisoning-attack-florida-shows-cybersecurity-gaps-water-systems-n1257173
[6] https://www.ksnt.com/news/local-news/kansas-hacker-pleads-guilty-to-shutting-down-drinking-water-plant-with-phone/
[7] https://itegriti.com/2022/compliance/waterisac-state-of-the-sector-2021-us-water-industry-in-hot-water-when-it-comes-to-cybersecurity/
[8] The term "operational technology" means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise. Internet of Things Cybersecurity Improvement Act of 2020, 15 U.S.C. § 271(3)(6) (Public Law 116-207).

EPA is committed to partnering with co-regulators in the states[9] to ensure that all PWSs employ essential best practices for cybersecurity to protect public health. Water security planning has been a critical component of EPA and state efforts to ensure the provision of clean and safe water since the increased threat of terrorism and malevolent attacks after 9/11. EPA and states have worked with PWSs to identify and protect against physical security vulnerabilities. Over the past twenty years, PWSs have increasingly relied on the use of electronic systems to operate drinking water systems efficiently. These electronic systems, however, have created a new vulnerability to cyber-attacks.

Today, PWSs are frequent targets of malicious cyber activity,[10] which has the same or even greater potential to compromise the treatment and distribution of safe drinking water as a physical attack. Clarifying that cybersecurity must be evaluated in reviewing operational technology that is part of a PWS's equipment or operation during sanitary surveys or other state programs will help reduce the likelihood of a successful cyber-attack on a PWS and improve recovery if a cyber incident occurs.

The definition of sanitary survey is "an onsite review of 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."[11] Pursuant to relevant regulatory requirements, states are required to conduct periodic sanitary surveys of PWSs.[12] As further explained in the Addendum below, EPA interprets the regulatory requirements relating to the conduct of sanitary surveys to require that when a PWS uses operational technology, such as an industrial control system (ICS),[13] as part of the equipment or operation of any required component[14] of a sanitary survey, then the sanitary survey of that PWS must include an evaluation of the adequacy of the cybersecurity of that operational technology for producing and distributing safe drinking water.

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. EPA's existing guidance documents[15,16] and the integration of computerized processes in modern PWSs highlight the importance of incorporating cybersecurity in sanitary surveys.

Accordingly, during a sanitary survey of a PWS, states must do the following to comply with the requirement to conduct a "sanitary survey:"

---

[9] "State" in this memo means the definition in 40 Code of Federal Regulations (CFR) § 141.2, which is "the agency of the State [including territories] or Tribal government which has jurisdiction over public water systems."
[10] Alert (AA21-287A), Ongoing Cyber Threats to U.S. Water and Wastewater Systems, https://www.cisa.gov/uscert/ncas/alerts/aa21-287a
[11] 40 CFR § 141.2
[12] 40 CFR § 141.2, 142.16(b)(3), 142.16(o)(2).
[13] An *industrial control system* is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems, used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. (NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/ics)
[14] 40 CFR § 142.16(b)(3) and (o)(2) [required components are listed in the Addendum]
[15] USEPA 2019a, *How to Conduct a Sanitary Survey of Drinking Water Systems,* EPA 816-R-17-001; available at: https://www.epa.gov/dwreginfo/sanitary-surveys
[16] USEPA 2019b, *Sanitary Survey Field Reference for Use When Conducting a Sanitary Survey of a Small Water System,* EPA 816-R-17-002; available at: https://www.epa.gov/dwreginfo/sanitary-surveys

(1) If the PWS uses an ICS or other operational technology as part of the equipment or operation of any required component of the sanitary survey, then the state must evaluate the adequacy of the cybersecurity of that operational technology for producing and distributing safe drinking water.
(2) 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.[17]

EPA has defined "significant deficiencies" as including, but not limited to, "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."[18] For cybersecurity, significant deficiencies should include the absence of a practice or control, or the presence of a vulnerability, that has a high risk of being exploited, either directly or indirectly, to compromise an operational technology used in the treatment or distribution of drinking water.

States can fulfill the responsibility to evaluate cybersecurity through different approaches, such as those described in Section 1 below, conducted under their sanitary survey programs. Alternatively, states may meet this requirement by using an existing or establishing a new program outside of sanitary surveys that is no less stringent than federal regulations and involves identifying and addressing significant deficiencies in cybersecurity practices at PWSs.[19] States retain their existing flexibility with sanitary surveys in how they evaluate PWSs, identify significant deficiencies, and require PWSs to address significant deficiencies.

This memorandum concerns the assessment and improvement of cybersecurity of operational technology at PWSs through sanitary surveys or alternative state programs. It does not encompass all components necessary for a comprehensive critical infrastructure cybersecurity program, such as potential state roles in cyber incident reporting and response.

Section 1. Approaches to Include Cybersecurity in PWS Sanitary Surveys

EPA recognizes that several states have already established programs to evaluate PWS cybersecurity practices and to assist PWSs with protecting against cyber threats. Other states may have less capacity to assist communities sufficiently in building protections against cyber threats. To account for the differences among states in their capacity and capability, EPA is providing information on different approaches states could employ to evaluate cybersecurity at PWSs. In addition, states may want the flexibility to use different approaches based on the circumstances of individual PWSs, as well as to transition from one approach to another as capacity and capability change over time.

<u>Option 1: Self-assessment or third-party assessment of cybersecurity practices</u>

States that have or establish the requisite authority may require PWSs to conduct a self-assessment of cybersecurity practices for the purpose of identifying cybersecurity gaps (i.e., the absence of recommended cybersecurity practices or controls or presence of vulnerabilities).

[17] 40 CFR § 142.16(b)(1)-(3) and (o)(1)-(2)
[18] 40 CFR § 142.16(o)(2)(iv)
[19] Under SDWA Section 1413, 42 U.S.C. § 300g-2, states with primary enforcement responsibility (primacy) do not have to adopt drinking water regulations identical to EPA's national primary drinking water regulations. Rather, primacy states must adopt drinking water regulations that are "no less stringent" than EPA's national primary drinking water regulations, meaning that these states have a certain degree of flexibility in attaining and maintaining primacy.

Option 1.a. Self-Assessment. PWSs could conduct this assessment using a government or private-sector method approved by the state, such as those from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA),[20] National Institute of Standards and Technology (NIST),[21] American Water Works Association (AWWA),[22] International Organization for Standardization (ISO,[23] and International Society of Automation/International Electrotechnical Commission (ISA/IEC).[24] In guidance published with this memorandum for public comment, described in Section 2, EPA is providing an optional method that PWSs (or states) may use to conduct an assessment with a checklist of recommended cybersecurity practices and controls.

Option 1.b. Third-Party Assessment. Alternatively, a PWS could undergo an assessment of cybersecurity practices by an outside party, EPA's Water Sector Cybersecurity Evaluation Program,[25] or another government or private sector technical assistance provider approved by the state. EPA is expanding its capacity to assist states and PWSs with conducting assessments.

Under Options 1.a and 1.b, the cybersecurity assessment for the PWS, whether it is a self-assessment or one conducted by a third party, should be completed prior to the sanitary survey, made available to state sanitary surveyors, and then updated to reflect changes in cybersecurity practices and/or operational technology prior to subsequent sanitary surveys. During the sanitary survey, the state surveyor should confirm completion of the assessment and determine whether identified cybersecurity gaps are significant deficiencies. As described in Section 2, EPA guidance provides examples and recommendations for states to consider when identifying a cybersecurity significant deficiency. Further, states and PWSs may consult with EPA for technical assistance once cybersecurity gaps are identified.

States may also require PWSs to develop follow-on risk mitigation plans to address cybersecurity gaps identified during the assessment, specifically including any significant deficiencies if designated by the state. The risk mitigation plan would list planned mitigation actions and schedules. The state would review the risk mitigation plan during the sanitary survey, ensure that the PWS is taking necessary steps to address any significant deficiencies if designated by the state, and offer to identify additional resources PWSs could use to address those gaps.

PWSs should complete the risk mitigation plan prior to their sanitary survey and update it, as necessary, prior to subsequent sanitary surveys. EPA guidance includes recommended actions for addressing cybersecurity gaps and a template for a risk mitigation plan. EPA technical assistance is also available to consult with states and PWSs regarding cybersecurity risk mitigation actions and plans.

<u>Option 2: State evaluation of cybersecurity practices during the sanitary survey</u>

States could choose for surveyors to evaluate cybersecurity practices directly during a sanitary survey of a PWS to identify cybersecurity gaps and determine if any of those gaps should be designated as significant deficiencies. This approach is consistent with how states conduct sanitary surveys of other components of PWS operations. Under this option, the state, rather than the PWS or a third party, would

[20] CISA *Cyber Resilience Review*, https://www.cisa.gov/uscert/resources/assessments
[21] NIST *Cybersecurity Framework*, https://www.nist.gov/cyberframework
[22] AWWA, *Cybersecurity Assessment Tool and Guidance*, https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
[23] ISO, *27001 Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html
[24] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[25] EPA *Water Sector Cybersecurity Evaluation Program*, https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program

conduct the cybersecurity assessment and would direct the PWS to address any significant deficiencies that the state identifies. EPA training and technical assistance on evaluating cybersecurity in PWS sanitary surveys is available to assist states that take this approach as well.

Option 3: Alternative State Program for Water System Cybersecurity

Several states have programs under which PWSs assess cybersecurity gaps (which might be called "security gaps," "vulnerabilities," or their equivalent) in their current practices that could impact safe drinking water and implement controls to address those gaps. For example, a state homeland security agency may have a cybersecurity program covering all critical infrastructure in the state. Another example is a state emergency management agency that conducts the cybersecurity assessment for the PWS instead of or in collaboration with the state agency responsible for the PWS supervision program. States that currently have or that develop such a program may use this program as an alternative to including cybersecurity in PWS sanitary surveys. PWSs serving Rural Communities with populations of less than 10,000 can utilize U.S. Department of Agriculture (USDA) Rural Development (RD) funded technical assistance providers. These communities may also already have requirements to complete cyber security analysis as part of loan and grant terms with USDA RD. To be at least as stringent as a sanitary survey, state surveyors must ensure that the alternate state programs effectively identify cybersecurity gaps (or equivalent) through an assessment and that PWSs address any significant deficiencies if designated by the state. Further, the cybersecurity assessment must be conducted at least as often as the required sanitary survey frequency for the PWS (typically 3 or 5 years).

Changes to State Recordkeeping and Reporting

Because this memorandum does not change the *Code of Federal Regulations*, it does not require states to revise their approved state primacy programs.[26] If the state approves an agent other than the state to conduct the cybersecurity component of a sanitary survey at a PWS, as described under Option 1, the state must maintain a list of the approved agent(s).[27] States must include cybersecurity in their annual evaluation of the state's program for conducting sanitary surveys that states report to EPA.[28] For groundwater systems, states must maintain records of written notices of significant deficiencies and confirmation that a significant deficiency has been corrected.[29] States must report to EPA the date a groundwater system completed the corrective action.[30] States are not required to report the significant deficiency itself to EPA.

Section 2: EPA Technical Assistance for Cybersecurity in PWS Sanitary Surveys

EPA is providing guidance, training, and technical assistance as described below to help states and PWSs include cybersecurity in sanitary surveys. These resources, as well as additional information from EPA on PWS cybersecurity, are available here: EPA Cybersecurity Best Practices for the Water Sector | US EPA.[31] Section E of the addendum lists additional resources that can assist states and PWSs with evaluating cybersecurity and addressing deficiencies.

[26] 40 CFR § 142.12
[27] 40 CFR § 142.14(a)(5)(ii)(F)
[28] 40 CFR § 142.15(c)(5)
[29] 40 CFR § 142.17(d)(i) and (iii)
[30] 40 CFR § 142.15(c)(7)(ii)
[31] https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector

Guidance Documents

In support of this memorandum, EPA is providing guidance to states and PWSs to assist in the evaluation of cybersecurity at PWSs during sanitary surveys. With today's memo, EPA has published a guidance document, *Evaluating Cybersecurity in PWS Sanitary Surveys*, for public comment. This guidance includes an optional checklist of cybersecurity practices that could be used to:

- assess cybersecurity at a PWS,
- identify gaps, including potential significant deficiencies, and
- select remediation actions appropriate to the capabilities and circumstances of the PWS.

This checklist directly reflects the CISA *Cross-Sector Cybersecurity Performance Goals*.[32] It includes recommended practices and controls to enhance the security and resilience of operational technology against cyber-attacks. It also includes recommended practices that PWSs could voluntarily implement to improve the cybersecurity of information technology networks that are connected to the PWS operational technology. The guidance has an optional template for a cybersecurity risk mitigation plan.

Additional guidance topics include the protection of security-sensitive information (also addressed in the Addendum below), potential funding, technical assistance resources for states and PWSs, and frequently asked questions (FAQs). The use of all EPA guidance by PWSs and states is optional. EPA also continues to encourage PWSs to use available government and private-sector cybersecurity assessment methods, such as those listed under Option 1 of this memorandum.

Training

In 2023, EPA will offer training for states and PWSs on evaluating cybersecurity in sanitary surveys. Like the guidance, the training will cover approaches to evaluate cybersecurity practices at a PWS, including identifying gaps and potential significant deficiencies, actions that PWSs could employ to address cybersecurity gaps, information protection, available technical assistance from EPA and other public and private-sector organizations, and potential funding.

All training will be provided virtually with recorded versions available. In-person training may be provided as well. Training will be offered separately for states in each EPA Region. For PWSs, training will be available nationally. For all trainings, EPA will strive to ensure state approval of Continuing Education Credits/Units (CECs/CEUs).

Technical Assistance

EPA has set up the *Cybersecurity Technical Assistance Program for the Water Sector*.[33] Under this program, states and PWSs can submit questions or request to consult with a subject matter expert (SME) regarding cybersecurity in PWS sanitary surveys, such as identifying whether a cybersecurity gap is a significant deficiency or selecting appropriate risk mitigation actions. EPA will strive to have an SME respond to the questioner within two business days. All assistance will be remote (phone or email as appropriate). The technical assistance service will not be an emergency line to report cyber incidents and it will not serve as a resource for cyber incident response or recovery efforts (users will be directed to the appropriate federal contact for these issues).

[32] https://www.cisa.gov/cpgs
[33]https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities

EPA's *Water Sector Cybersecurity Evaluation Program*[34] will carry out an assessment of cybersecurity practices at PWSs. The assessment will follow the Checklist in the guidance document, *Evaluating Cybersecurity in PWS Sanitary Surveys*. The PWS will receive a report with responses to Checklist questions that shows gaps in cybersecurity, including potential significant deficiencies. The PWS should provide this report to the state to review during the sanitary survey, as discussed under Option 1 of this memorandum. To participate in this program, a PWS must register at https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program.

ADDENDUM: SUPPLEMENTARY INFORMATION ON ADDRESSING PWS CYBERSCURITY IN SANITARY SURVEYS OR AN ALTERNATE PROCESS

This addendum provides supplementary information related to the memorandum. In addition to the technical assistance available from EPA, as described in the memorandum, this addendum can help states and PWSs understand the need to address cybersecurity in PWS sanitary surveys and locate more resources that can assist with this effort.

A. *Does EPA's interpretation regarding cybersecurity and sanitary surveys apply to me?*

This interpretation applies to all states, territories, and tribes that have jurisdiction over PWSs. During any period when a state, territorial, or tribal government does not have primary enforcement responsibility pursuant to Section 1413 of the Safe Drinking Water Act, the term "state" means the Regional Administrator, U.S. Environmental Protection Agency. As indicated above, the use of "state" in this memorandum encompasses this definition.

B. *What action is the EPA taking?*

EPA is interpreting its existing regulations regarding the duties of states during PWS sanitary surveys, which states are required to perform under 40 CFR §§ 141.2, 142.16(b)(3) and 142.16(o)(2). This action does not change the text of the *Code of Federal Regulations* (CFR).

The definition of a sanitary survey is stated in the memorandum above. Sanitary surveys must include an evaluation of each of the following components as applicable within the required survey frequency (described in section G below): (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, and (8) operator compliance with state requirements.[35]

Under 40 CFR Sections 141.723(c)-(d) (for sanitary surveys conducted by EPA), 142.16(b)(1)(ii) -(iii) (for surface water systems), and 142.16(o)(2)(v) (for ground water systems), a PWS must take necessary corrective actions to address any significant deficiencies identified by the state in sanitary survey reports. As described in this memo, this requirement applies to any significant deficiencies identified in sanitary survey reports (or an equivalent alternate state-approved process, as described in this memo) regarding the cybersecurity of any operational technology used by the PWS as part of its equipment or operation for producing and distributing safe drinking water.

[34] https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program
[35] 40 CFR §§ 142.16(b)(3) and 142.16(o)(2)

EPA's guidance documents support this interpretation of the regulatory text. Most notably, EPA already interprets its sanitary survey regulations to require a review of Supervisory Control and Data Acquisition (SCADA)[36] systems.[15,16] These SCADA systems have been integral to the operation of many PWSs since the inception of EPA's sanitary survey regulations and cyberattacks on these SCADA systems have the demonstrated potential to disrupt the delivery of safe drinking water. Given the importance of SCADA systems to the production and distribution of safe drinking water at many PWSs and existing sanitary survey guidance calling for their general review, providing that such review encompass cybersecurity aspects of these systems is justified and logical.

In addition, because the concept of physical security is already a component of EPA guidance on sanitary surveys,[15,16] incorporating the review of cybersecurity is logical, particularly where essential SCADA systems are expected to face cybersecurity threats. Finally, EPA guidance already recommends that sanitary surveys review emergency response plans,[15,16] and such plans are required to account for cybersecurity under Safe Drinking Water Act (SDWA) Section 1433. Thus, existing sanitary survey guidance already points to cybersecurity considerations because such considerations are contained, by law, within emergency response plans.

Evaluating cybersecurity is also consistent with the purpose of sanitary surveys. Broadly, sanitary surveys aim to "evaluate the adequacy of the system, its sources and operations and the distribution of safe drinking water."[37] Malicious cyber activity incidents have been demonstrated to impact PWSs' ability to deliver safe drinking water. Given the importance of cybersecurity to the safe functioning of a PWS's operational technology, evaluating the cybersecurity of the operational technology affecting a PWS's "equipment" and "operation" fits within the definition, context, and purpose of sanitary surveys. Sanitary surveys are a preventative tool to identify threats to public health before they materialize, and cybersecurity is clearly preventative.

Sanitary surveys must evaluate those aspects of the PWS within the eight required components that are necessary for the production and distribution of safe drinking water. Based on the integral nature of cybersecurity-vulnerable SCADA systems in the equipment and operation of modern drinking water systems, a sanitary survey that does not evaluate cybersecurity is not appropriately evaluating the adequacy of the system to produce and distribute safe drinking water. Cybersecurity is essential to the adequate operation of modern PWSs, fits squarely within the systems' "equipment," and "operation," and therefore is an integral part of sanitary surveys under existing EPA regulations.

C. *Why is EPA communicating this interpretation now?*

The use of operational technology, including industrial control systems like SCADA, in the production and distribution of drinking water has become widespread among PWSs of all sizes and types. These control systems have allowed PWSs to reduce onsite staffing and to operate collection, treatment, and distribution system processes more efficiently. Notably, they permit remote monitoring and operation by offsite personnel, including third parties.

However, operational technology is also vulnerable to being disabled or manipulated through malicious cyber activity, which is occurring with increasing frequency. Documented malicious cyber activity has utilized various techniques, such as stolen credentials from authorized users, malicious URLs and

[36] "SCADA" is "a computerized system that is capable of gathering and processing data and applying operational controls over long distances." (NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition)
[37] 40 CFR § 142.16(b)(3) and (o)(3)

websites, vulnerabilities in software applications, compromised third party software and service providers, insecure remote access systems, insider attacks, and others. Intrusion by a cyber threat actor into an operational technology network can compromise the ability of a water system to produce and/or distribute safe drinking water. For example, incidents of malicious cyber activity on PWSs have shut down critical treatment processes, locked up control system networks behind ransomware, and disabled communications used to monitor and control distribution system infrastructure like pumping stations.[38]

CISA manages the National Cyber Awareness System, which issues alerts of cyber threats to critical infrastructure networks, including water systems.[39] This information builds awareness among critical infrastructure owners and operators of recently discovered cybersecurity exploits and vulnerabilities. These alerts demonstrate that critical infrastructure networks are threatened frequently by attempted cyber intrusions carried out by sophisticated threat actors. These exploits can disrupt the operations of PWSs and other critical infrastructure facilities. However, the mitigation strategies in these alerts show that cybersecurity best practices, such as those in the NIST *Cybersecurity Framework*,[40] can be effective in reducing the risk of many of these attacks.

EPA's interpretation of its regulations supports the agency's mission to work with states, territories, tribes, and EPA's many partners to protect public health through safe drinking water. It recognizes the increasingly critical role of operational technology in the production and distribution of drinking water at many PWSs and the vulnerability of operational technology to cyber-attacks. The state has an essential role in overseeing the delivery of safe drinking water under its jurisdiction. Including cybersecurity in sanitary surveys or equivalent alternate programs builds awareness and heightens oversight of this important practice area for PWSs. By identifying and addressing significant deficiencies in cybersecurity practices through PWS sanitary surveys, the risk of a cyber-attack degrading safe drinking water can be reduced. For these reasons, EPA is providing this interpretation now.

D. *How does this interpretation relate to America's Water Infrastructure Act of 2018?*

America's Water Infrastructure Act of 2018 (AWIA) amended the SDWA to require community water systems serving over 3,300 people to, among other actions, assess the risk and resilience of "electronic, computer, or other automated systems (including the security of such systems)."[41] AWIA further requires each system to "prepare or revise, where necessary, an emergency response plan," which must "include strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system."[42] AWIA, however, 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. In addition, AWIA has no comparable requirements for community water systems serving 3,300 people or fewer or for any non-community water systems (approximately 140,000 water systems).

The interpretation in this memo significantly builds upon the public health protections in AWIA. First, this interpretation applies to all PWSs, rather than the subset of community water systems subject to AWIA. Second, when a state evaluates or reviews (in the case of a 3rd party assessment) the adequacy of

[38] Hassanzadeha et al. 2020, *A Review of Cybersecurity Incidents in the Water Sector*, Journal of Environmental Engineering, 146.
[39] https://us-cisa.gov/ncas/alerts
[40] https://www.nist.gov/cyberframework
[41] SDWA Section 1433(a)(1)(A)(i)
[42] SDWA Section 1433(b)(1)

the cybersecurity of operational technology for producing and distributing safe water, the state provides an assessment or review that is independent of the one performed by the water system under AWIA. Third, if the state identifies a significant deficiency in cybersecurity during a sanitary survey or equivalent alternate program, the PWS must take necessary corrective action to address the deficiency, which is not the case for risks or other vulnerabilities identified by a water system under AWIA.

Finally, there is nothing in the AWIA amendments that limits EPA's requirement that states must address cybersecurity in PWS sanitary surveys or equivalent alternate programs. PWSs that developed risk and resilience assessments and emergency response plans under AWIA may use these documents to support the evaluation of cybersecurity during their sanitary surveys.

E. *What additional cybersecurity resources are available to states and PWSs?*

Section 2 of the memorandum describes technical assistance available from EPA to help states and PWSs evaluate cybersecurity during sanitary surveys and address gaps, including significant deficiencies. This assistance includes guidance, training, the *Water Sector Cybersecurity Evaluation Program* and the *Water Sector Technical Assistance Service*. Additional technical and financial resources that can help states and PWSs with cybersecurity in sanitary surveys are listed below.

Technical resources

- Section 1 of the memorandum lists examples of government and private sector methods in addition to EPA's that may be used to evaluate cybersecurity practices at PWSs and identify actions to address cybersecurity gaps.
- The NIST *Cybersecurity Framework*[43] is a comprehensive voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. NIST offers guidance and resources to assist critical infrastructure owners and operators with using the *Cybersecurity Framework* to manage their cyber risks.
- DHS CISA is a primary source of resources for critical infrastructure cybersecurity. CISA offers a broad array of tools, guidance, and services to strengthen the security and resilience of critical infrastructure facilities against cyber-attacks[44]. For example, CISA products can help PWSs to identify cybersecurity vulnerabilities, develop proactive mitigation strategies that lower the cybersecurity risk of operational technology, and take steps to counter pervasive threats like ransomware.
- CISA Cybersecurity Advisors (CSAs), who are located in the ten CISA regional offices,[45] offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal and territorial governments. CSAs act as liaisons to CISA cyber programs, along with other public and private resources. CSAs can assist with cyber preparedness, assessments and protective resources, partnership in public-private development, and cyber incident coordination and support.
- The United States Department of Agriculture (USDA) Rural Development Circuit Rider program provides technical assistance, including cybersecurity analysis, to rural water systems serving 10,000 people or less. [46] Rural water system officials may request assistance from the National Rural Water Association State Association or the local Rural Utilities Service office. Circuit Riders provide service in all states and territories.

[43] https://www.nist.gov/cyberframework
[44] https://www.cisa.gov/cybersecurity
[45] https://www.cisa.gov/cisa-regions
[46] https://www.rd.usda.gov/programs-services/water-environmental-programs/circuit-rider-program-technical-assistance-rural-water-systems

- The Water Information Sharing and Analysis Center (ISAC)[47] is a source for data, case studies, and analysis on water security threats, including cybercrime, and provides resources to support response, mitigation, and resilience initiatives.
- The Multi-State ISAC supports information sharing to improve the overall cybersecurity of state, local, tribal, and territorial governments; assists cyber incident response and remediation; and issues advisories with actionable information for improving cybersecurity.[48]
- Water sector private associations, including the American Water Works Association[49] and National Rural Water Association[50] offer cybersecurity education, guidance, and methods to assess cybersecurity risks and prioritize cybersecurity enhancements that are targeted specifically to PWSs.

Financial resources

- EPA manages the Drinking Water State Revolving Fund (DWSRF) loan fund and set-asides, which may be used to support state programs and communities with cybersecurity controls.[51]
- EPA's Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program is a new grant program for public water systems serving more than 10,000 people to support projects that increase resilience to natural hazards, cybersecurity vulnerabilities, or extreme weather events.
- The USDA Rural Utilities Service Water and Environmental Programs provide loans, grants, and loan guarantees, as well as technical assistance, to PWSs in rural communities of 10,000 people or less for infrastructure and infrastructure improvements, which include cybersecurity upgrades.[52]
- The DHS State and Local Cybersecurity Grant Program, managed jointly by CISA and the Federal Emergency Management Agency (FEMA), helps state, local, and territorial governments across the country address cybersecurity risks and threats to information systems that they own or that are operated on their behalf.[53,54]

F. *Can sensitive information about cybersecurity practices be protected from disclosure?*

Withholding from public disclosure information about specific cybersecurity practices and vulnerabilities at PWSs may be necessary due to the potential for this information to be exploited to facilitate a cyber intrusion or attack on the PWS.

In some cases, sanitary surveys are performed by EPA regional offices as the primacy agency for a particular state or area (Wyoming, the District of Columbia, most Indian Tribes). EPA may also perform cybersecurity assessments through the Technical Assistance Provider Program (per Section 1). The Agency plans to assert applicable Freedom of Information Act (FOIA) exemptions to withhold sensitive portions of any sanitary survey report or PWS cybersecurity assessment held by EPA, including portions that deal with a PWS's cybersecurity practices if such a report is requested under FOIA. Applicable exemptions under FOIA for withholding such information may include Exemption 4 (confidential

[47] https://www.waterisac.org/
[48] https://www.cisecurity.org/ms-isac
[49] https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
[50] https://nrwa.org/issues/cybersecurity/
[51] https://www.epa.gov/sites/default/files/2019-10/documents/cybersecurity_fact_sheet_final.pdf
[52] https://www.rd.usda.gov/programs-services/water-environmental-programs
[53] https://www.cisa.gov/cybergrants
[54] https://www.epa.gov/system/files/documents/2022-12/221121-SLCGP_508c.pdf

business information or CBI) and Exemption 7(f) (law enforcement records whose disclosure could reasonably be expected to endanger the life or physical safety of any individual).

For sanitary surveys conducted by a state, tribal, or territorial government, the applicable laws of the government entity that holds the report will govern the withholding of sensitive cybersecurity information from public disclosure. Most states have adopted information protection laws like FOIA under state law,[55] and EPA recommends that states withhold such sensitive information if requested to the extent allowable under state law. State requirements for reporting information to EPA related to evaluating cybersecurity in sanitary surveys are discussed in Section 1 of the memorandum.

EPA guidance and training discussed in Section 2 of the memo include recommendations to states on potential approaches to identify and segregate cybersecurity information in sanitary survey reports that should be withheld from public disclosure. For example, states concerned about their authority to withhold sensitive cybersecurity information from public disclosure may take the following steps, if consistent with applicable state law:

- Sanitary surveyors may leave assessments of cybersecurity practices, the identification of cybersecurity gaps, mitigation plans, and other sensitive information with the PWS. The state would not hold this information.
- Official surveyor reports could be limited to confirming that the cybersecurity assessment was performed, whether gaps were identified, including significant deficiencies, and the schedule for corrective actions if needed. Information on specific gaps and significant deficiencies would be left with the PWS (not included in the state report or otherwise held by the state). The state surveyor would review progress in correcting significant deficiencies during virtual or onsite follow-ups.
- Where allowed, surveyors could keep detailed notes on PWS cybersecurity vulnerabilities and related information in internal, non-public documents that are not subject to public disclosure requirements.

G. *What are the additional requirements for PWS sanitary surveys?*

Requirements for PWS sanitary surveys are described in 40 CFR parts 141 and 142. This memorandum interprets but does not modify or add to the existing requirements, which are summarized here. For a more complete description of these requirements, see *How to Conduct a Sanitary Survey of Drinking Water Systems*.[56]

The baseline sanitary survey frequency is every three years for community water systems and every five years for non-community water systems.[57] The frequency can be reduced to every five years for community water systems that have an outstanding performance record, as determined by the state, or for ground water systems that provide 4-log treatment (99.99 percent reduction) of viruses before the first customer[58] (non-community water systems using only protected and disinfected ground water must

[55] *Protecting the Water Sector's Critical Infrastructure Information, Analysis of State Laws*, American Water Works Association, 2020. https://www.awwa.org/Portals/0/AWWA/Government/ProtectingtheWaterSectorsCriticalInfrastructureInformation.pdf
[56] https://www.epa.gov/sites/default/files/2019-08/documents/sanitary_survey_learners_guide_508_8.27.19.pdf
[57] See 40 CFR §§ 142.16(b)(3) and 142.16(o)(2))
[58] See id.

undergo subsequent sanitary surveys at least every 10 years). The components of a sanitary survey may be completed as part of a staged or phased state review process within the established frequency.[59] A "significant deficiency" is defined in 40 CFR Section 141.723 for sanitary surveys conducted by EPA and 40 CFR Section 142.16(o)(2)(iv) for ground water systems (the definition is stated above in the memorandum). For PWSs using surface water sources, the state must describe how it will decide whether a deficiency identified during a sanitary survey is significant in its application for primacy.[60]

H. *Did EPA engage stakeholders on this topic before issuing the memorandum?*

In June 2022, EPA and the Association of State Drinking Water Administrators (ASDWA) convened a workgroup of representatives from state and tribal drinking water agencies to discuss evaluating cybersecurity in PWS sanitary surveys. Over the course of five virtual meetings, as well as on a draft workgroup report, EPA solicited comments from the workgroup on potential approaches. Prior to this workgroup, in June 2021, EPA discussed the use of sanitary surveys to assess cybersecurity with ASDWA to solicit its leadership's initial feedback on the policy approach. Subsequently in 2021, EPA engaged in individual discussions with the leadership and staff of each of the major drinking water sector associations to seek their input on this approach. EPA also participated in such discussions with the Water Sector Coordinating Council and Water Government Coordinating Council throughout 2022. EPA derived valuable insight from these engagements, which the Agency has incorporated into the memorandum and guidance.

[59] See id.
[60] 40 CFR § 142.16(b)(3)(v)