JS|HELD

PERSPECTIVES

Water Cybersecurity? EPA Mandates Regulations to Prevent Cyberattacks on Public Water Systems

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

EPA AIMS TO MITIGATE RISK OF CYBERATTACK ON PUBLIC WATER SYSTEMS

On March 3, 2023, the U.S. Environmental Protection Agency (EPA) issued its Memorandum Addressing Public Water System (PWS) Cybersecurity in Sanitary Surveys or an Alternate Process to expand state audits of water systems to include an evaluation of operational technology cybersecurity. The memorandum states, "While PWSs have taken important steps to improve their cybersecurity, a recent survey 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 cyber-attack—whether from an individual, criminal collective, or a sophisticated state or state sponsored actor." The memorandum was issued a day after the White House released a comprehensive cybersecurity plan aimed at mitigating breach threats to government agencies, industry, schools, hospitals, and other key infrastructure.

WHY IS THIS IMPORTANT AND WHO IS IMPACTED?

Public Water Systems are the primary source of drinking water for approximately 90% of all Americans. Under the Safe Drinking Water Act (SDWA), public water systems are regulated by the EPA. The EPA establishes and enforces standards to ensure the safety of everyone's drinking water. One of the several items that are mandated by the SDWA is the annual Consumer Confidence Report. That report which must be sent to all customers includes the following information:

- The lake, river, aquifer, or other source of the drinking water.
- A brief summary of the risk of contamination of the local drinking water source.
- The regulated contaminant found in local drinking water.
- The potential health effects of any contaminant detected in violation of an EPA health standard.
- An accounting of the system's actions to restore safe drinking water.
- An educational statement for vulnerable populations about avoiding Cryptosporidium.
- Educational information on nitrate, arsenic, or lead in areas where these contaminants may be a concern.
- Phone numbers of additional sources of information, including the water system.
- EPA's Safe Drinking Water Hotline number 1-800-426-4791.

There are approximately 155,693 public water systems in the United States.[1] They are classified in three tiers:

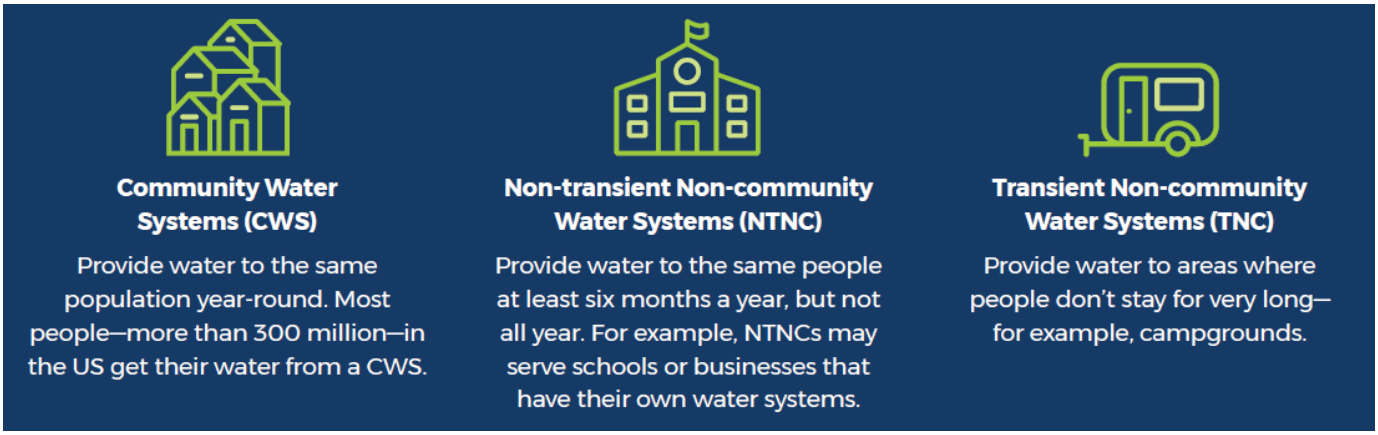

Figure 1 *- U.S. public water system types (Source: EPA).*

[1] https://www.cdc.gov/healthywater/drinking/public/index.html

In 2007, for example, over 286 million Americans received their tap water from a community water system. Below is a description of how water systems work. In the last several years, information technology systems have been increasingly built into this process to enhance treatment and delivery. However, introduction of technology also presents potential risk.

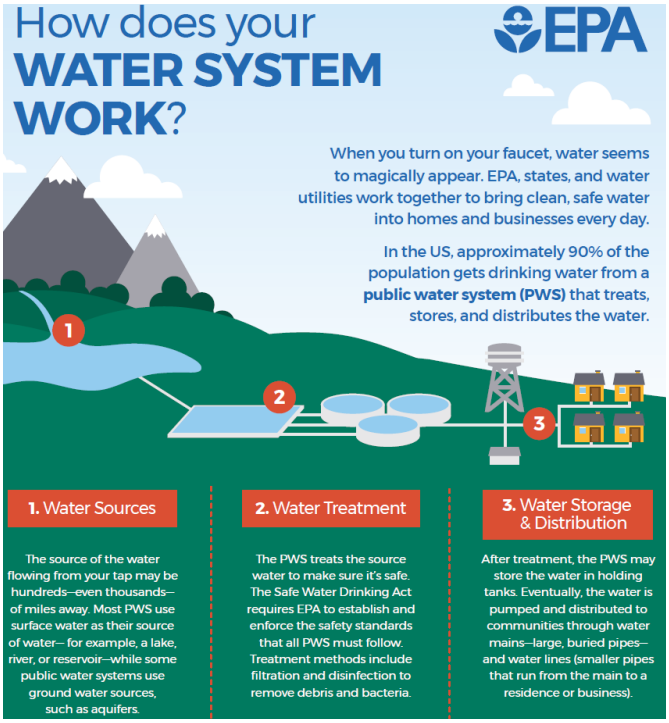

***Figure 2** - How public water systems work (Source: EPA).*

Infrastructure elements, including water processing and delivery, have traditionally struggled with the concept of integrating information technology (IT) with operational technology (OT). This integration becomes even more challenging with the introduction of "Internet of Things" (IOT) devices added to the PWS ecosystem. These IT and OT advancements, including industrial control systems and supervisory control and data acquisition systems (ICS/SCADA), which can automate many elements of OT and improve the ability to monitor and control, can also increase risk. The potential risk is not just a systems breach but the interruption of critical services vital to our country, including power, telecommunications, roadways, and, yes, water. Like other government and municipal entities, water utilities have budget limitations. Accordingly, introducing new IT that requires ongoing updates, monitoring, and maintenance, necessitates additional investment to defend against public safety and national security threats to these critical infrastructure elements. It is a horrible day when corporate America is attacked. It can be deadly if water supplies are impacted.

WHAT IS THE REGULATORY BASIS FOR THE NEW CYBERSECURITY REQUIREMENT?

Under the authority of the SDWA, 40 CFR § 142.16(b)(3) and (o)(2) already required states to conduct periodic audits or "sanitary surveys" of PWSs. In particular, the regulations require that these sanitary surveys include "an onsite review of the water source (identifying sources of contamination using results of source water assessments where available), facilities, equipment, operation, maintenance, and monitoring compliance of a public water system to evaluate the adequacy of the system, its sources and operations, and the distribution of safe drinking water." 40 CFR § 142.16(b)(3). The EPA's memorandum states that the new cybersecurity evaluation requirement merely clarifies what is meant to be included in the onsite review of "equipment" and "operation." It is through this interpretation—and not any modification of existing regulations—that the EPA will now require states to include a cybersecurity review when conducting sanitary surveys. EPA's memorandum identifies different approaches for states to fulfill this responsibility and provides a list of questions they may use in conducting the assessment.

HOW WILL THE STATES CONDUCT CYBERSECURITY REVIEW?

The memorandum allows states to adopt one of three options for incorporating cybersecurity review into PWS sanitary surveys. As shown in the table below, states may utilize 1) PWS or third-party assessment, 2) state evaluation during the sanitary survey, or 3) an existing state water system

cybersecurity program that is at least as stringent as a sanitary survey. Importantly, if a state allows PWSs to conduct their own cybersecurity evaluations or hire a third party, the assessment must be completed prior to the state sanitary survey. The state may also require the PWS to develop a risk mitigation plan prior to the sanitary survey to address any cybersecurity gaps that are identified during a self-assessment. Any method used for self-assessment would need to be conducted using a government or other state-approved method. Any private third party conducting the assessment would similarly need to be approved by the state.

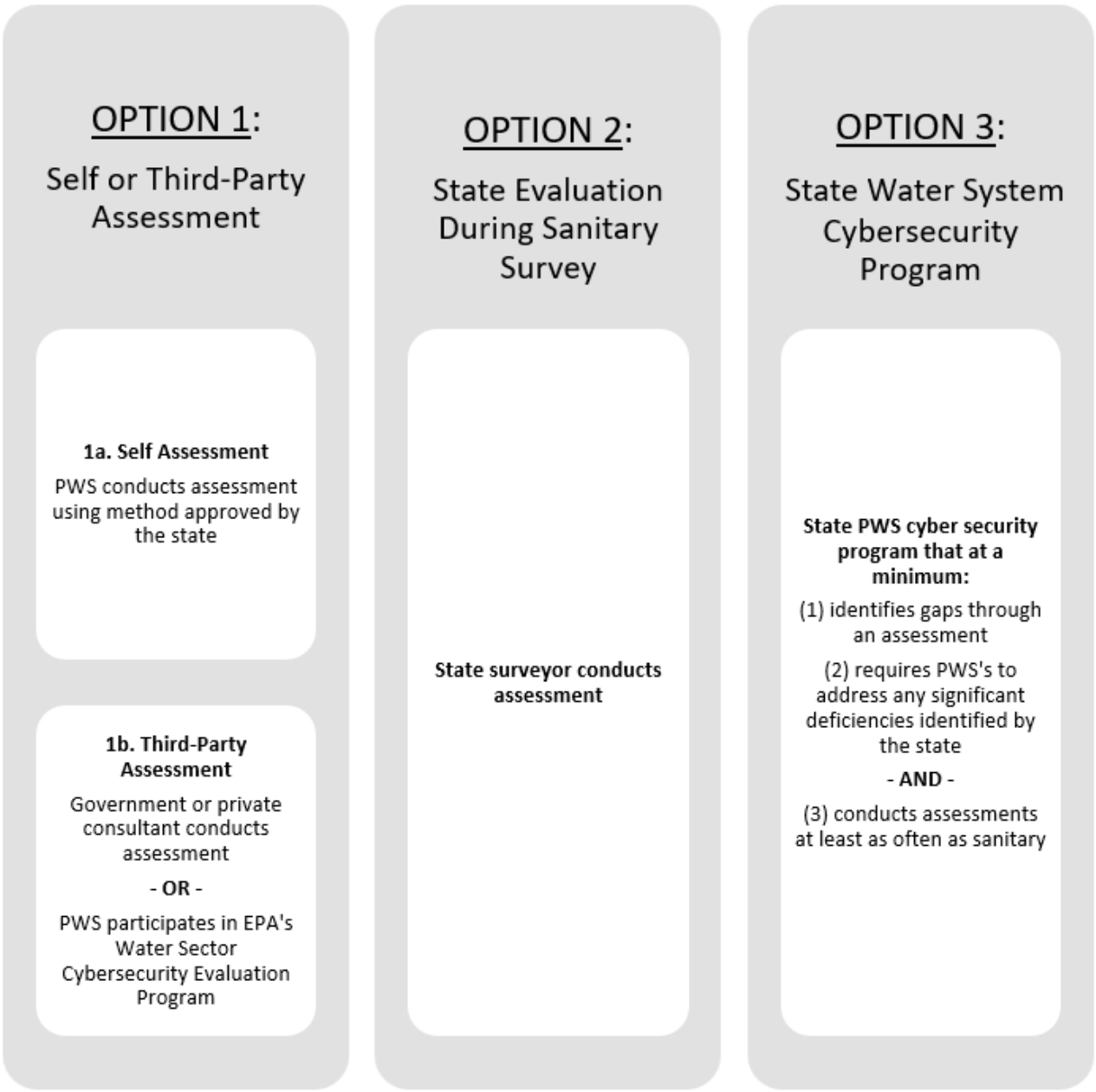

Figure 3 *- Options for incorporating cybersecurity review into PWS sanitary surveys.*

WHAT IS THE IMMEDIATE INDUSTRY RESPONSE TO THE MEMORANDUM?

Industry response to the EPA's new cybersecurity assessment requirement for PWSs has been mixed. Mike Hamilton, former chief security officer for the City of Seattle, commented that limiting approved assessment methodology to government or state-approved methods "make[s] this activity hard to scale across the breadth of water utilities across the country." Tracy Mehan, executive director of government affairs at the American Water Works Association, similarly warns that the plan puts states in a tough position by directing that cybersecurity reporting should start immediately.

Integration of the EPA's new cybersecurity assessment into PWS operations may depend on the current state of the utility. Facilities with integrated IT and OT that have any outward or public facing network elements likely already have a robust cybersecurity program. If not, they will likely have a steep hill to climb to successfully complete the EPA's mandated cybersecurity assessment and will need to begin securing their networks expeditiously. If IT and OT are still separated, there may be less risk of a significant gap now being identified during state sanitary surveys, but this does not mean that immediate action will not still be necessary; rather, the potential impact of a cyberattack is segregated based on the isolated nature of the OT environment. Action to protect internet facing network elements will still be required. If a utility cannot bill or track service, it is effectively shut down, which may present a public safety or national security threat.

Conversely, reliance on the EPA's memorandum alone may not be enough to secure the nation's water supply. Tied to the current requirements for community and non-community state sanitary surveys, PWS cybersecurity assessments will be necessary once every three or five years, or more frequently where appropriate. Cybersecurity good practices typically suggest more frequent and ongoing assessment.

WHAT CAN PWSs DO NOW TO ACCELERATE COMPLIANCE WITH THE NEW REQUIREMENT?

With its memorandum, EPA provides an optional checklist that states may use during a sanitary survey to evaluate the cybersecurity of a PWS's operational technology. Prior to the rule coming into effect, if a state does not elect to implement a self- or third-party assessment, PWSs should give serious consideration to this checklist and take steps to develop a plan that includes creating internal accountability and conducting an informal cybersecurity review sufficiently in advance of any upcoming sanitary survey to allow for implementation of corrective good practices prior to state assessment. Additional guidance can be found in the EPA publication, "Evaluating Cybersecurity During Public Water System Sanitary Surveys."

For some PWSs, this will be starting from scratch. They should start with the EPA checklist (shown below) and other free tools available to establish a picture of the current state and begin working on enhancing their ability to defend against and respond to cyberattack. PWSs can also look to trusted third party consultants to help them down this path.

Account Security	• Does the PWS detect and block repeated unsuccessful login attempts? • Does the PWS change default passwords? • Does the PWS require multi-factor authentication wherever possible, but at a minimum to remotely access PWS operational technology ("OT") networks? • Does the PWS require a minimum length for passwords? • Does the PWS separate user and privileged accounts? • Does the PWS require unique and separate credentials for users to access OT and IT networks? • Does the PWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?

Device Security	• Does the PWS require approval before new software is installed or deployed? • Does the PWS disable Microsoft Office macros, or similar embedded code, by default on all assets? • Does the PWS maintain an updated inventory of all OT and IT network assets? • Does the PWS prohibit the connection of unauthorized hardware to OT and IT assets? • Does the PWS maintain current documentation detailing the set-up and settings of critical OT and IT assets?
Data Security	• Does the PWS collect security logs to use in both incident detection and investigation? • Does the PWS protect security logs from unauthorized access and tampering? • Does the PWS use effective encryption to maintain the confidentiality of data in transit? • Does the PWS use encryption to maintain the confidentiality of stored sensitive data?
Governance & Training	• Does the PWS have a named role/position/title that is responsible and accountable for planning, resourcing, and execution of cybersecurity activities within the PWS? • Does the PWS have a named role/position/title that is responsible and accountable for planning, resources, and execution of OT-specific cybersecurity activities? • Does the PWS provide at least annual training for all PWS personnel that covers basic cybersecurity concepts? • Does the PWS offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties? • Does the PWS offer regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?
Vulnerability Management	• Does the PWS patch or otherwise mitigate known vulnerabilities within the recommended time frame? • Does the PWS ensure that assets connected to the public Internet expose no unnecessary exploitable services? • Does the PWS eliminate connections between its OT assets and the Internet?
Supply Chain/Third Party	• Does the PWS include cybersecurity as an evaluation criterion for the procurement of OT assets and services? • Does the PWS require that all OT vendors and service providers notify the PWS of any security incidents or vulnerabilities in a risk-informed timeline?
Response & Recovery	• Does the PWS have a written procedure for reporting cybersecurity incidents, including how and to whom? • Does the PWS have a written cyber security incident response plan for critical threat scenarios which is regularly practiced and updated? • Does the PWS have backup systems necessary for operations on a regular schedule, store backups separately from the source systems, and test backups on a regular basis? • Does the PWS maintain updated documentation describing network topology across PWS OT and IT networks?
Other	• Does the PWS segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed? • Does the PWS keep a list of threats and adversary tactics, techniques, and procedures for cyberattacks relevant to the PWS and have the capability to detect instances of key threats? • Does the PWS use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?

HOW TO PREPARE YOUR PWS TO COMPLY WITH THE EPA'S NEW CYBERSECURITY REQUIREMENTS

Professionals with expertise in Environmental Compliance audits and program evaluation, Enterprise Risk Management program development and evaluation, and Cyber Security risk assessment and mitigation can help impacted organizations prepare for compliance. Additionally, the right experts can provide custom operational, programmatic, and governance-oriented solutions, assisting a PWS in beginning the journey toward enhanced cyber security, including developing a roadmap to compliance with EPA's new cybersecurity requirements prior to future state sanitary surveys.

ACKNOWLEDGMENTS

We would like to thank our colleagues Kim Logue, John F. Peiserich, and Ron J. Yearwood, Jr., CISSP, CISM, CIPM for insights and expertise that greatly assisted this research.

Kim Logue is an Associate Vice President in J.S. Held's Environmental, Health & Safety – Risk & Compliance group. Ms. Logue specializes in environmental risk and compliance. With over 15 years of experience in the areas of environmental and natural resources law, Ms. Logue provides consulting and expert services for industrial facilities and law firms throughout the country. She has extensive experience with assessing and managing potential and ongoing compliance obligations with innovative client-focused strategies. Ms. Logue conducts environmental compliance audits, advises clients on the development of effective environmental management systems, and conducts due diligence associated with mergers and acquisitions. She routinely supports clients on rulemaking and legislative efforts focused on environmental and natural resources issues.

Kim can be reached at Kim.Logue@jsheld.com or +1 504 561 6563.

John Peiserich is a Senior Vice President in J.S. Held's Environmental, Health & Safety - Risk & Compliance group. With over 30 years of experience, John provides consulting and expert services for heavy industry and law firms throughout the country with a focus on Oil & Gas, Energy, and Public Utilities. He has extensive experience evaluating risk associated with potential and ongoing compliance obligations, developing strategies around those obligations, and working to implement a client-focused compliance strategy. Mr. Peiserich has appointments as an Independent Monitor through EPA's Suspension and Debarment Program. John routinely supports clients in a forward-facing role for rulemaking and legislative issues involving energy, environmental, Oil & Gas, and related issues.

John can be reached at john.peiserich@jsheld.com or +1 504 360 8373.

Ron Yearwood is a Senior Managing Director in J.S. Held's Digital Investigations and Discovery group. Mr. Yearwood has more than 30 years of experience combatting the foremost criminal and national security threats. Mr. Yearwood has substantial experience advising and collaborating with clients on incident response, cybersecurity preparedness/resiliency/risk mitigation, and complex investigations. Having spent more than 23 years with the Federal Bureau of Investigation (FBI), Mr. Yearwood led strategic and investigative operations against hundreds of criminal and nation state cyber threat actors. During his tenure in the FBI Cyber Division, Mr. Yearwood served as a representative to the White House Cyber Response Group.

Ron can be reached at ron.yearwood@jsheld.com or +1 904 375 7792.