FACT SHEET

Addressing Cybersecurity Resilience with Sanitary Surveys

Cyber-attacks against water systems are increasing. These attacks have the potential to disable or contaminate the delivery of drinking water to consumers. While some public water systems (PWSs) have taken important steps to improve their cybersecurity, many PWSs have failed to adopt basic cybersecurity best practices and consequently are at risk of being victimized by a cyber-attack. EPA is committed to partnering with the states to ensure that all PWSs adopt cybersecurity practices that are essential to protecting public health.

What must primacy agencies do during a Sanitary Survey?

1. If the PWS uses an Industrial Control System 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.

Available Options for Primacy Agencies to Include Cybersecurity in Sanitary Surveys

Option 1: PWSs conduct self-assessment or third-party assessment of cybersecurity practices

Option 1.a. Self-Assessment: PWSs could conduct a state-approved self-assessment using a government or private-sector method, such as those listed below.

Option 1.b. Third-Party Assessment: A PWS could undergo an assessment of cybersecurity practices by an outside party, such as those listed below, or another government or private sector technical assistance provider approved by the state.

Under Options 1.a and 1.b, the PWS cybersecurity assessment should be completed prior to the sanitary survey, made available to state sanitary surveyors, and updated to reflect changes in cybersecurity practices and/or operational technology prior to subsequent sanitary surveys.

Self-Assessment Resources:

- EPA: Guidance on Evaluating Cybersecurity in Public Water System Sanitary Surveys
- CISA: Cyber Resilience Review, Cross-Sector Cybersecurity Performance Goals
- NIST: AXIO Cybersecurity Program Assessment Tool
- AWWA: Cybersecurity Risk Management Tool
- ISO: ISO/IEC 27001
- ISA/IEC: ISO 62443 Series of Standards

Third-Party Assessment Resources:

- CISA: CISA Cybersecurity Advisor (Coordinated though CISA Regions)
- EPA: Water Sector Cybersecurity Evaluation Program

Option 2: Primacy agency evaluation of cybersecurity practices during the sanitary survey

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 conduct the cybersecurity assessment and would direct the PWS to address any significant deficiencies that the state identifies. Please see the list of resources below to support states with this approach. Note: States may also use the self-assessment tools listed under Option 1.

Resources available to support this approach:

- EPA: Cybersecurity Assessment Tool and Risk Mitigation Plan Template
- EPA: Cybersecurity Technical Assistance Program for the Water Sector

Option 3: Alternative State Program for Water System Cybersecurity

Several states have programs under which PWSs assess cybersecurity gaps 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. States that currently have or that develop such a program may use this program as an alternative to including cybersecurity in PWS sanitary surveys. To be at least as stringent as a sanitary survey, state surveyors must ensure that the alternate state programs effectively identify cybersecurity gaps through an assessment and 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).

Identifying Significant Deficiencies

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. Primacy agencies with additional questions on identifying significant deficiencies can submit a request for additional support at *www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities*.

Changes to Primacy Agency Recordkeeping and Reporting

This interpretive rule does not require states to change their approved state primacy programs.

1. If PWS cybersecurity assessments are completed by an agent other than the Primacy Agency, the Primacy Agency must maintain a listing of approved agent(s).

2. Primacy Agencies are not required to report the significant deficiency itself to EPA, but must report to EPA the date a system completed the corrective action.

EPA Resources for Primacy Agencies and Public Water Systems

Guidance on Evaluating Cybersecurity in PWS Sanitary Surveys

Evaluating Cybersecurity in PWS Sanitary Surveys is a guidance document that includes an optional checklist of
cybersecurity best practices that could be used to:

- Assess cybersecurity at a PWS
- Identify gaps, including potential significant deficiencies
- Select remediation actions appropriate to the capabilities and circumstances of the PWS.

Training for State Primacy Agencies and Public Water Systems

EPA will offer training for states and PWSs on evaluating cybersecurity in sanitary surveys. Please register for the training at *https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector*

Virtual Sanitary Survey Cybersecurity Training for Primacy Agencies:

This training will provide primacy agencies with an understanding of how to implement cybersecurity into sanitary surveys using Option 1, 2, or 3. It will also cover information protection, available support resources, and funding.

Regional Sanitary Survey Cybersecurity Training for Primacy Agencies:

This training will be conducted in-person and provide primacy agencies with an understanding of how to implement cybersecurity into sanitary surveys using Option 1, 2, or 3. It will also cover state-specific cybersecurity requirements, information protection, available support resources, and funding.

Virtual Cybersecurity Assessment Training for Public Water Systems:

This training will provide PWS staff with a detailed overview on how to conduct a cybersecurity self-assessment, identify vulnerabilities, and develop risk mitigation plans to prioritize, address, and mitigate the vulnerabilities found during the assessment. It will also cover information protection, available support resources, and funding.

EPA Direct Technical Assistance for Primacy Agencies and Public Water Systems

Water Sector Cybersecurity Evaluation Program

EPA's Water Sector Cybersecurity Evaluation Program will conduct a cybersecurity assessment for PWSs. The assessment will follow the Checklist in the guidance on *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. PWSs must register at *https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program*.

Cybersecurity Technical Assistance Program for the Water Sector

EPA has launched a new technical assistance program to support primacy agencies and water systems in implementing cybersecurity measures. Users may submit questions or request to consult with a subject matter expert regarding cybersecurity in PWS sanitary surveys. EPA will strive to have a response to the requester within two business days. Submit a request at *http://www.epa.gov/waterriskassessment/ forms/cybersecurity-technical-assistancewater-utilities*.

Note: This service is not intended to provide emergency support. For support following a cyber incident, please report to the appropriate state authority and/or CISA at the following: *https://us-cert.cisa.gov/forms/report*

Additional Technical Resources

- **CISA Cybersecurity Advisors (CSAs)**: CSAs offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal and territorial governments. CSAs can assist with cyber preparedness, assessments and protective resources, partnership in public-private development, and cyber incident coordination and support. To locate your CSA email *cyberadvisor@hq.dhs.gov*.
- **United States Department of Agriculture (USDA) Rural Development Circuit Rider Program**: USDA provides technical assistance, including cybersecurity analysis, to rural water systems serving 10,000 people or less. 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. For more information, visit *www.rd.usda.gov/programs-services/waterenvironmental-programs/circuit-riderprogram-technical-assistance-rural-water-systems*
- **Water Information Sharing and Analysis Center (ISAC)**: WaterISAC 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. For more information, visit *www.waterisac.org*.
- **Multi-State ISAC**: MS-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. For more information visit *http://www.cisecurity.org/ms-isac*

- **Water Sector Associations**: The American Water Works Association and National Rural Water Association offer cybersecurity education, guidance, and methods to assess cybersecurity risks and prioritize cybersecurity enhancements that are targeted specifically to PWSs.

For more information: *www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector*