Commonwealth of Massachusetts
Executive Office of Energy & Environmental Affairs

Department of Environmental Protection
100 Cambridge Street Suite 900 Boston, MA 02114 • 617-292-5500

Maura T. Healey
Governor

Kimberley Driscoll
Lieutenant Governor

Rebecca L. Tepper
Secretary

Bonnie Heiple
Commissioner

December 28, 2023

IMPORTANT NOTICE
Your PWS 2024 Sanitary Surveys and
Cybersecurity Program/Assessment Report Inspection Reminder

Dear Public Water Supplier:

The Massachusetts Department of Environmental Protection (MassDEP) Drinking Water Program (DWP) records indicate that your public water system (PWS) is scheduled for a sanitary survey in 2024. **MassDEP will also inspect your cybersecurity assessment findings and plans during the sanitary survey.**

MassDEP/DWP considers cybersecurity as part of the routine operations and maintenance of a PWS to ensure the continuous delivery of safe drinking water. Public Water Suppliers must address Cybersecurity in their Emergency Response Plan (ERP) as it can be an act of vandalism or sabotage that has the potential to impact the quality or quantity of water available to the system [310 CMR 22.04(13)(a)9)]. **MassDEP/DWP requires all PWS to have completed an assessment or maintain a cybersecurity plan/program unless the PWS does not have operational technology (OT) presenting a cybersecurity risk as described on the attached FAQ.**

Please review the MassDEP/DWP and USEPA resources on the attached Frequently Asked Questions (FAQ) and be prepared for MassDEP/DWP inspection of your water system's facilities, operations, and record-keeping including cybersecurity program/plan.

Your MassDEP regional office will contact you with specific information to schedule your 2024 sanitary survey. If you have any questions on this information, you may also contact the Drinking Water Program at program.director-dwp@mass.gov.

Thank you for your attention to this matter and your commitment to providing safe drinking water.

Sincerely,
Yvette DePeiza
Program Director,
MassDEP Drinking Water Program

eCC MassDEP/DWP Regional Section Chiefs
DWPArchive/ Sanitary Survey-Cybersecurity Inspection Reminder-12-28-2023

FREQUENTLY ASKED QUESTIONS AND RESOURCES

Which PWS must have Cybersecurity Assessments/Program/Plans?

All PWS with operational technology (OT) presenting a cybersecurity risk must have a cybersecurity plan/program or perform a cybersecurity assessment as part of their emergency planning responsibilities and have a subsequent plan to address all findings/gaps listed in their assessment report. OT equipment is defined as hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise. "OT equipment presenting a cybersecurity risk" include equipment that is or may occasionally be connected after initial installation:

- to a computer (for any reason including alarm reporting and patching) or
- to a network (local, wide area or internet), or
- is remotely accessible (either for control or monitoring)

Can a PWS use it EPA AWIA Risk and Resiliency Assessment (RRA) and Emergency Response Planning (ERP)?

Community Public Water Systems (CWS) serving a population of 3,300 or more can use their initial cybersecurity review performed for the 2018 America Water Infrastructure Act (AWIA) Section 2013 Risk and Resiliency Assessment (RRA) and Emergency Response Planning (ERP) requirements to meet the MassDEP/DWP requirement to perform a cybersecurity assessment or have a plan/program. The deadlines for the previous and upcoming AWIA RRA and ERP certifications are listed here: https://www.epa.gov/waterresilience/awia-section-2013#CD.

What if your PWS does not have any operational technology (OT) presenting a cybersecurity risk?

A PWS may determine that they do not have OT equipment presenting a cybersecurity risk. If a PWS makes that determination, it must provide MassDEP/DWP with its determination in writing by completing and returning the ERP-CS-OT form to MassDEP/DWP via email program.director-dwp@mass.gov, Subject: "Cybersecurity Assessment Operational Technology (OT) Not at a Cybersecurity Risk Statement - ERP-CS-OT", at the earliest convenience but not to exceed 30 days of receiving an initial notice from MassDEP to complete a cybersecurity assessment. MassDEP/DWP will contact/follow-up with all PWS that submit an ERP-CS-OT form. The Cybersecurity Statement-No OT Risks-ERP-CS-OT form can be found/downloaded at https://www.mass.gov/doc/cybersecurity-statement-no-ot-risks-erp-cs-ot/download.

Non-Community PWS

Transient Non-Community Water System (TNCs) and Non-Transient Non-Community Water System (NTNCs) may not have any operational technology (OT) presenting a cybersecurity risk as described above, but MassDEP will continue asking three basic questions during a sanitary survey to evaluate the cybersecurity posture of the PWS. If it is determined that the PWS has any OT-related risk conditions, they will need to complete a cybersecurity assessment.

Options for getting a Cybersecurity Assessment

PWS can receive an assessment by:

1. **USEPA Free Cybersecurity Assessment**: USEPA's free cybersecurity evaluation program: https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program,
2. **CISA Free Cybersecurity Assessment**: A free CISA cybersecurity assessment from can be arranged through the MassDEP or by contacting CISA's Massachusetts Cyber Security Analyst (CSA). If your PWS is interested in participating in free in person CISA assessment, please contact the Drinking Water Program at program.director-dwp@mass.gov: Subject: CISA Cybersecurity Assessment.

3. **Self or Consultant Cybersecurity Assessment:** Finally, a PWS can perform a free self-assessment using USEPA's Water Cybersecurity Assessment Tool: https://www.epa.gov/system/files/documents/2023-03/EPA%20Water%20Cybersecurity%20Assessment%20Tool%201.0_0.xlsx or arrange for outside consultants to perform assessments using other accepted approaches, including those utilizing the National Institute of Standards and Technology (NIST CSF), the International Society of Automation/International Electrotechnical Commission standard 62443 (ISA 62443), the International Organization for Standards/ International Electrotechnical Commission standard 27001 (ISO 27001), and the American Water Works Association Cybersecurity Assessment Tool (AWWA).

Protecting Sensitive Information

The cybersecurity assessment report* includes sensitive information please do not email the report to anyone, including MassDEP.

*Please be aware that the Massachusetts Public Records Law - MGL c. 4, § 7(26) contains provisions that exempt certain records from disclosure, see https://www.sec.state.ma.us/divisions/public-records/download/guide.pdf . Your cybersecurity assessment reports contain sensitive information that must be protected from disclosure.

Cybersecurity Resources

MassDEP/DWP Cybersecurity Posters and Information: https://www.mass.gov/info-details/public-drinking-water-system-operations#cybersecurity-
MassDEP- PWS Cybersecurity Incident Response Plan Template: https://www.mass.gov/doc/cybersecurity-incident-response-template/download
EPA Cybersecurity Webpage: https://www.epa.gov/waterresilience/cybersecurity-assessments

Sanitary Survey Resources

MassDEP: https://www.mass.gov/doc/preparing-for-a-sanitary-survey-0/download
USEPA: https://www.epa.gov/dwreginfo/sanitary-surveys