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

June 28, 2023

IMPORTANT NOTICE
ON SANITARY SURVEYS AND CYBERSECURITY ASSESSMENTS

Dear Public Water Suppliers,

On March 3, 2023, the USEPA released an important memorandum on cybersecurity to State Drinking Water Administrators[i]. The memorandum included the following directives to states:

- **Cybersecurity assessments of public water systems (PWS) must be part of sanitary surveys or other approved state programs.**
- **PWS must correct identified cybersecurity deficiencies/vulnerabilities/gaps**.
- **States and PWSs can evaluate the cybersecurity of PWS using one of the three options:**
  - USEPA provided free cybersecurity assessment,
  - PWS self-assessment, or
  - Third-party assessment using approved USEPA alternatives.

Information on the USEPA memorandum was provided in the MassDEP/DWP "Cybersecurity, Emergency Preparedness and You" section of the March 10, 2023, *In the Main* Newsletter. See https://www.mass.gov/doc/in-the-main-drinking-water-program-updates-03-10-2023/download.

The MassDEP Drinking Water Program (DWP) considers cybersecurity to be a **vital and routine** part of Emergency Response Plan (ERP) requirements pursuant to 310 CMR 22.04(13) and **expects all PWS to perform a cybersecurity assessment as part of their emergency planning responsibilities.** See MassDEP/DWP April 28, 2022, notice to PWS on ERP compliance at https://www.mass.gov/doc/notice-to-pws-emergency-response-plan-erp-checklist-required-to-document-erp-compliance/download.

MassDEP/DWP has taken a proactive approach in the past years to address this important issue by reminding PWS to perform ~~a~~ cybersecurity assessment and to address/correct all identified deficiencies/vulnerabilities. MassDEP/DWP has also included questions on cybersecurity in each sanitary survey and provided cybersecurity training and technical assistance information to all PWS in the DWP biweekly *In the Main* newsletter. See https://www.mass.gov/lists/communication-to-public-water-suppliers#newsletters-.

IMPORTANT NOTICE AND ACTION REQUESTED

1. **As part of the sanitary survey process, the findings of your cybersecurity assessment including any identified vulnerabilities/gaps/deficiencies will be reviewed to ensure that you are evaluating and addressing your system's cybersecurity needs and responsibilities.** These reviews will be conducted by MassDEP/DWP sanitary surveyors and/or cybersecurity technical assistance providers or partners (e.g., Cybersecurity and Infrastructure and Security Agency (CISA)). The review may be conducted on-site or through an alternate secure remote process, prior, during or after a sanitary survey or upon MassDEP/DWP request.
    a. Any unaddressed vulnerabilities/gaps/deficiencies identified during the review of your cybersecurity assessment report will be included in a cybersecurity section of the corrective action plan of the DEP/DWP sanitary survey report or in a subsequent update to your sanitary survey report, and
    b. You will be expected to correct and/or address and/or submit a plan to correct/address all unaddressed vulnerabilities/gaps/deficiencies identified in the cybersecurity assessment you provided for our review by the deadline specified in the corrective action plan.

    Please note: no details or sensitive cybersecurity information will be included in the sanitary survey report[ii]. For example, MassDEP/DWP will note the name and date of the PWS cybersecurity assessment report and refer to the page and item number of any unaddressed deficiencies/vulnerabilities or gap.

2. **If your system has already completed a sanitary survey this year OR will have one completed by year-end, to ensure that your system is prepared, MassDEP/DWP will be contacting you with additional information/steps regarding your cybersecurity assessments and the sanitary survey**.

3. **If you have not conducted a cybersecurity assessment, you may use any of the three USEPA identified cybersecurity assessment options**:
    a. USEPA provided free cybersecurity assessment,
    b. PWS self-assessment, or
    c. Third-party assessment using approved USEPA alternatives, such as a free assessment offered by CISA.

Note: Some small systems may not be vulnerable to cyber incidents because the PWS does not have operational technology (hardware or software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in your system) and if it does, the operational technology is not connected to a computer or to a network that is remotely accessible. If you believe that your system **is not** vulnerable to cyber incidents please contact MassDEP/DWP at program.director-dwp@mass.gov, Subject: Cybersecurity, **at your earliest convenience not to exceed 30 days of receiving this notice**. MassDEP/DWP will contact you upon receipt of your response.

MassDEP/DWP strongly recommend that you utilize the USEPA Free cybersecurity evaluation program if you need a cybersecurity assessment. See resources below.

CYBERSECURITY ASSESSMENT RESOURCES

USEPA Free Cybersecurity Evaluation Program: USEPA's free evaluation

USEPA's Cybersecurity Evaluation Program will conduct a cybersecurity assessment for PWS. The assessment will follow the checklist in the guidance on Evaluating Cybersecurity in PWS Sanitary Surveys which will then generate a report that will highlight gaps in cybersecurity, including potential significant deficiencies.

How to Apply: Use the following to apply today
https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program

Other Free Resources:

CISA Cyber Assessment CISA

How to Apply: Email CISA at vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started. For more details visit https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services.

Other Methods to Complete Your Cybersecurity Assessment:

- PWS may arrange for its own 3-party assessment (if the assessment includes all of the assessment criteria identified by USEPA and a section on vulnerabilities/ deficiencies or gaps, etc. or
- PWS may perform a self-assessment using the EPA's checklist/ WCAT tool or any of the following approved USEPA alternatives: NIST CSF, ISA 62443, ISO 27001, AWWA, and CISA RRA/CISA Assessment.

If you have any questions on this information, please contact the Drinking Water Program at program.director-dwp@mass.gov, Subject: Cybersecurity. Thank you for your attention to this matter, and your commitment to maintaining water system security and safe drinking water.

Sincerely,

Yvette DePeiza
Program Director,
MassDEP Drinking Water Program

[i] See https://www.epa.gov/newsreleases/epa-takes-action-improve-cybersecurity-resilience-public-water-systems

[ii] 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