



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

Date:«Date»

Attn: «Primary_Contact_Name»
«Physical_Address_»
«Email»

PWS City/Town: «TOWN»
PWS Name: «PWS_NAME»
PWS ID#: «PWSID»
Program: **Sanitary Surveys – Cybersecurity**

Dear Public Water Supplier:

Please find attached the Cyber Security Corrective Action Plan (CSCAP) summarizing the cybersecurity findings made during the sanitary survey of your system conducted on «Date».

The following staff attended the sanitary survey:

Affiliation	Name	Title/Role
PWS Representatives		
MassDEP DWP Representatives	Christopher Van Andrew Hildick-Smith Gufran Bulbul	Cybersecurity TAP Cybersecurity TAP Environmental Analyst

Please be advised that your system must update the Massachusetts Department of Environmental Protection (MassDEP) Drinking Water Program (DWP) on your public water system (PWS) plan of action to address the findings noted in this plan. Please review Tables A, B, and C and complete and submit Tables B, C and the signed certification of the CSCAP to program.director-dwp@mass.gov by «Deadline_for_CSCAP_Signed» .

If you have any questions regarding this cybersecurity review and the attached CSCAP, please contact MassDEP DWP at program.director-dwp@mass.gov. Subject: Cybersecurity.

Sincerely,

Yvette DePeiza
Program Director,
MassDEP Drinking Water Program

cc: File Copy - DWP Sanitary Survey-Cybersecurity
ecc: DWP Boston
Region: «Regional_Chief_» «Surveyor_»

File Name «PWS_NAME»: - «PWSID» - SS- Cybersecurity- «Date»

Re: Date: «Date»
PWS Name: «PWS_NAME»
PWS ID#: «PWSID»
Sanitary Survey- Cybersecurity
Type of PWS:
☒ COM over 3,300 in population

Security Sensitive - Not for Distribution

Massachusetts Department of Environmental Protection (MassDEP) considers cybersecurity to be a routine part of the operations and maintenance of a public water system (PWS) to ensure the continuity of safe drinking water and is also part of a PWS Emergency Response Plan (ERP) per 310 CMR 22.04(13). PWS must complete a cyber assessment and have a plan to address acts of vandalism or sabotage, including cyber incidences, that have the potential to impact the quality or quantity of water available to the system as required by 310 CMR 22.04(13)(a)9. **MassDEP also considers cybersecurity information to be sensitive and covered by MGL c. 4, § 7(26) cybersecurity waiver¹.**

SECTION I- INSPECTION

On «Date», MassDEP, as part of a Sanitary Survey inspected the above noted PWS cybersecurity assessment/ program based on the following item:

☒ Cybersecurity «Type_of_Assessment_». Cybersecurity Assessment Report: Date «Report_Dated»

SECTION II- FINDINGS AND ACTIONS

Based on the review/inspection of the information provided by the PWS MassDEP DWP has determined that in accordance with 310 CMR 22.04(13)(c) the PWS must address the inspection findings by the date(s) specified.

Attention: Please review Table A, B, and C. Complete/check all applicable boxes in Table B column 4, sign Section III certification, and return the completed Tables B, C and signed certification to MassDEP DWP at program.director-dwp@mass.gov by «Deadline_for_CSCAP_Signed». Please note: Failure to return Table B and the certification and address the findings may result in enforcement action.

Table A: IMMEDIATE ACTIONS TO BE COMPLETED

No immediate actions have been identified

Please see Tables B and C below

¹**Protect sensitive information:** Relevant Massachusetts Public Records Law
The Massachusetts Public Records Law - MGL c. 4, § 7(26) <https://www.sec.state.ma.us/divisions/public-records/download/guide.pdf>. Exemption (n) applies to: records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, **emergency preparedness**, threat or **vulnerability assessments**, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation, **cyber security** or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (c) of section 10 of chapter 66, is likely to jeopardize public safety or cyber security.

Table B: ACTION TO BE COMPLETED

This table lists any findings identified during the cybersecurity portion of the sanitary survey. PWS must update the MassDEP/DWP on your PWS plan of action to address the findings by completing and submitting this Table and the certification form to MassDEP/DWP by the date specified in the column 3 below. **Please only submit a completed Table B and refrain from sharing additional documents or sensitive information.**

1 Citation	2 Findings	3 MassDEP Deadline	4 Action(s) Completed By PWS, Date(s)
310 CMR 22.04(13)(c)	Findings as identified in the cybersecurity assessment report dated «Report_Dated».	By «Deadline for CSCAP Signe d», confirm your intent to address all findings by completing column 4 with the timeline of your plan. Submit this completed Table B and signed certification to MassDEP Drinking Water Program program.director-dwp@mass.gov, Subject CSCAP. To protect sensitive data your PWS email response should not include any sensitive information.	On or by _____ my PWS will take/took the following checked action(s): A. ☐ My PWS addressed all identified areas of concerns/findings and incorporated all applicable recommendations listed in the report. Or B. ☐ My PWS addressed findings that required immediate attention. And ☐ My PWS will address all remaining identified areas of concern/findings and incorporate all applicable recommendations listed in the report: ☐ Within one year of date on CSCAP ☐ Within two years of date on CSCAP ☐ Before the MassDEP/DWP next sanitary survey schedule And ☐ My PWS will notify MassDEP /DWP in writing (with the statement “All cybersecurity items addressed”) at program.director-dwp@mass.gov, Subject: CSCAP, when all findings have been addressed. To protect sensitive data your PWS email response should not include any sensitive information.

The following items are recommended to improve your PWS cyber program and ability to provide safe drinking water. These items may be elevated to Table B findings in subsequent surveys. **Please indicate your PWS plan of action for the following recommendations by checking the boxes for each recommendation your PWS plans to take or utilize.**

Table C: RECOMMENDATIONS

MassDEP/DWP Recommendations	PWS Planned Actions
Apply for MassDEP DWP Cybersecurity Improvement Grant: https://www.mass.gov/info-details/public-water-suppliers-cybersecurity-improvements-grant-program	☐
MassDEP DWP Self-Paced Course on Basic Cybersecurity Measures for Water and Wastewater Systems in Massachusetts (1 TCH) - Enroll Here Free: https://classes.wateroperator.org/courses/cybersecurity	☐
Sign up for the federal Cybersecurity and Infrastructure Security Agency (CISA) no cost vulnerability scanning subscription service: https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning	☐
Apply Today for Municipal Cybersecurity Awareness Grant Program (MCAGP) and Receive Free Cybersecurity Training for Your Staff https://www.mass.gov/info-details/municipal-cybersecurity-awareness-grant-program	☐
Free Cybersecurity Health Check Program- Office of Municipal and School Technology (OMST) https://www.mass.gov/info-details/cybersecurity-health-check-program	☐

Use MassDEP/DWP PWS Cyber incident plan Template - https://www.mass.gov/doc/cybersecurity-incident-response-template/download	☐
The Mass Cyber Center: MA Municipalities-Cyber Resilient Massachusetts Grant Program. Learn More & Apply Here: Notice of Funding Opportunity for Cyber Resilient Massachusetts Grant Program MassTech	☐
Sign up for Multi-State Information Sharing and Analysis Center (MS-ISAC)- Free for U.S. State, Local, Tribal & Territorial Government Entities https://www.cisecurity.org/ms-isac	☐
Use the EPA Water Utility Response On-The-Go Plus Mobile Application- tool designed for water utilities responding to emergency incidents including cybersecurity: https://www.epa.gov/waterutilityresponse/water-utility-response-go-plus-mobile-application	☐
Review the cybersecurity attachment in the MassDEP/DWP biweekly newsletter. This newsletter includes important information, including security updates, resources, and alerts https://www.mass.gov/info-details/in-the-main#cybersecurity,-emergency-preparedness,-and-you!-	☐
Review MassDEP/DWP Cybersecurity Resource Hub : Include resources and alerts for PWS to improve cybersecurity defenses, mitigate cyber-attack risks, and enhance overall resiliency and compliance.	☐
MassDEP/DWP posters with cybersecurity tips to inform your staff and help keep your systems secure https://www.mass.gov/info-details/public-drinking-water-system-operations#cybersecurity-	☐
Join MassWARN at https://www.mawarn.org/	☐
ICS Security Training – Idaho National Lab. https://inl.gov/national-security/ics-cybersecurity-training	☐
Other: _____	☐

SECTION III- Certification

I certify under penalties of law that I am the person authorized to fill out this form and the information contained herein is true, accurate, and complete to the best extent of my knowledge and my PWS will annually update MassDEP DWP when changes are made to our ERP including cybersecurity by completing the form <https://www.mass.gov/doc/emergency-response-plan-erp-compliance-checklist/download> and submitting it along with our Annual Statistical Report required by 310 CMR 22.15(5)e.

Water Commissioner, Owner, Owner Representative, or Other Responsible Party:

Signature: _____ Date: _____

Print Name: _____ Title: _____

Section IV- For MassDEP DWP Use