|  | Massachusetts Department of Environmental Protection ERP-CS-OT  Bureau of Water Resources – Drinking Water Program  **Emergency Response Plan (ERP) Compliance – Cybersecurity Assessments -Operational Technology (OT) is Not at a Cybersecurity Risk Statement** | | | |
| --- | --- | --- | --- | --- |
| **Important:** When filling out forms on the computer, use only the tab key to move your cursor - do not use the return key. | Information and Instructions  All public water systems (PWS) that have operational technology (OT) that is connected to a computer or to a network that is remotely accessible, must complete a cybersecurity assessment and be ready to present the cybersecurity assessment report during the sanitary survey process or as requested by MassDEP/DWP. Operational Technology (OT) is considered hardware or software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the system.  **Note:** This form must be completed if PWS believe the above OT conditions do NOT apply. Please review the certification statements below. **To submit this form, all certification statements must be checked.**  If a PWS determines that it does not have OT cybersecurity risks, it may still participate in the MassDEP cybersecurity program to improve its Information Technology (IT) cybersecurity. In which case there is no need to return this form. | | | |
|  | A. System Information | | | |
| MassDEP/DWP strongly encourages all PWS to routinely check and ensure that their cybersecurity program is up-to date.  **Resources:**  [EPA: Water Sector Cybersecurity Evaluation Program](https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program):  [EPA Technical Assistance Program (Subject Matter Experts):](https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector)  [CISA No-Cost Vulnerability Scanning Subscription Service](https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning): | PWS Name | | | Date |
| PWS ID # | | | City /Town |
| PWS Type:  COM  NTNC  TNC | | | |
| Mailing Address | | | |
| Phone | FAX | E-mail | |
| B. Certification  My PWS understands that cybersecurity is a vital and routine part of Emergency Response Plan (ERP) requirements pursuant to 310 CMR 22.04(13) and all Massachusetts’ PWS are expected to assess and eliminate cybersecurity vulnerabilities as part of their emergency response planning responsibilities. This includes performing routing cybersecurity operations and maintenance practices to ensure the security of our systems, such as:   * Ensuring the PWS ERP is regularly updated and the PWS is routinely monitoring for potential security threats. * Providing staff with training to recognize, respond and report cyberattacks. * Keeping all computers, devices, and applications updated and current. * Enforcing the use of strong passwords and enabling multifactor authentication.   My PWS acknowledges that if a subsequent evaluation of our system by MassDEP/DWP (such as during an inspection, sanitary survey, or any other informational review) indicates a need for a cybersecurity assessment, our PWS will be required to conduct a cybersecurity assessment and report the results to MassDEP/DWP within 60 days of MassDEP notification of the need to conduct a cybersecurity assessment.    I certify that our PWS OT (hardware or software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the system) **is not at a cybersecurity risk because it meets all three of the following conditions**:  It is **not** currently or occasionally **connected to a computer** (for any reason including alarm reporting and patching),  It is **not** currently or occasionally **connected to a network** (local, wide area or internet), and  It is **not** currently or occasionally **remotely accessible** (either for control or monitoring). | | | |
| My PWS has made the above determination using the following type of assessment/tool:  Self-assessment, Date:  EPA assessment, Date:  CISA assessment, Date:  other, describe:     , Date:  I certify under penalty 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 of my knowledge and belief. | | | |
| |  |  | | --- | --- | | Print Name of Responsible Party | Title | | Signature | Date |   *If you have any questions on this information, or your need technical assistance, please contact the Drinking Water Program at* [*program.director-dwp@mass.gov*](mailto:program.director-dwp@mass.gov)*, Subject: Cybersecurity.*  *Section* | | | |
|  | C. For MassDEP/DWP USE ONLY | | | |