YES, NO or NA

The purpose of this document is to provide guidance on preparing a Wastewater Treatment Facility (WWTF) Cybersecurity plan document ("the plan") to the Rhode Island Department of Environmental Management (DEM) for review and approval. Ensuring each of these items are addressed during the planning process will help to expedite DEM's review and approval. Refer to the *Rules and Regulations for the Operation and Maintenance of Wastewater Treatment Facilities (250-RICR-150-10-4)* and Section 4.4, Section 4.5(H), and Section 4.6(B) for additional details

Note: This checklist should be completed through a collaborative effort between the facility and their cybersecurity services provider (the Town or third-party services).

The plan takes into consideration the recommendations from the National Institute of Standards and Technology Cybersecurity Framework and National Preparedness Goals, focusing on the core functions of:

Govern: The WWTF's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
Identify: The WWTF's current cybersecurity risks are understood
Protect: Safeguards to manage the WWTF's cybersecurity risks are used.
Respond: Actions regarding a detected cybersecurity incident are taken.
Recover: Assets and operations affected by a cybersecurity incident are restored.

The following items are required as part of the submittals:

1. A digital/hardcopy of emergency response and emergency communications during a substantial cybersecurity incident
    a. Verbal notification to RI DEM within twenty-four (24) hours from the discovery of a substantial cybersecurity incident.
        i. This step can be included in a facility's communication plan.
2. Incident Response Plan
    a. In the event of a substantial cyber incident, who is immediately notified, immediate actions, and what are the general interim operating measures
    b. Incident Response Plan and Emergency Communication Plan should be reviewed annually (and updated if needed)
3. Risk Management Plan
    a. The facility must submit a cover letter with the date of the last full asset inventory of operational technology (OT) and information technology (IT) assets and who led the inventory assessment.
    b. Considers critical component and system design life
    c. When the facility is made aware of a vulnerability, who do they inform and how is action taken.
    d. Does the facility employ any of the following basic Cyber Hygiene Practices
        i. A timely offboarding program that will limit digital and physical access to facility assets once employment ends.
        ii. Default passwords on new equipment (PLCs, Routers, etc.) are changed upon installation at the facility/collection system
        iii. Employee passwords and credentials are updated/changed semi-annually.

YES, NO or NA

iv. Key facility programs, databases, and systems employ multifactor authentication.
v. All facility staff have required annual cybersecurity training.

4. If facility has SCADA, …
    a. Evaluate facility's capability of operating without SCADA (staffing, sampling, operations, process control)
    b. Are there controls in place to limit off-site access to SCADA?
5. Physical Security
    a. Critical assets adequately secured
    b. Door locks, security cameras, etc. are functional
6. Limit connections to the Internet, especially for OT critical process/devices (Strongly recommend)
7. Add list of recommendations following June 2022 TTX.
    a. Prohibit connection of unauthorized devices (Strongly Recommend)

The plan shall include a schedule of implementation for short-term (within the following two years) and long-term (beyond two years) actions/projects.