CONFIDENTIAL

DO NOT COPY

DO NOT RELEASE FOR PUBLIC REVIEW

Cybersecurity Vulnerability Assessment for

Public Water System Name:

_____

Public Water System I.D. Number:

NY _____

Prepared by: _____

Title: _____

Signature: _____

Date Completed: _____

Confidential Information "This report may contain information that if disclosed could endanger the life or safety of the public, and therefore, pursuant to section seven hundred eleven of the executive law, this report is to be maintained and used in a manner consistent with protocols established to preserve the confidentiality of the information contained herein in a manner consistent with law."

Implementing cybersecurity best practices is a critical component to safeguarding a drinking water utilities ability to deliver clean, safe water. Cyberattacks are a growing threat to critical infrastructure sectors, including water systems.

The questions in the following checklist have been mapped back to components of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0) that you will find at the end of each question. It contains components which consist of standards, guidelines, and practices to promote the protection of critical infrastructure. Informative references are also provided for each component of the *Framework*. Additional information on the *Framework* is available at: https://www.nist.gov/cyberframework.

Process control systems (PCS), such as supervisory control and data acquisition (SCADA) systems, operate and monitor various functions at many water treatment, distribution and storage facilities. Examples of PCS functions include operating pumps and valves, monitoring and transmitting storage tanks levels, and recording and storing regulatory monitoring data.

Business enterprise systems encompass all other systems not used to operate and monitor water treatment and distribution. Examples include systems used for: email and internet access; customer accounts, meter reading, and billing; water system websites; and other administrative functions.

Please select the best answer to each question. If your answer is No, include a corrective action and target completion date. If you answer not applicable (N/A), explain why this is so for your facility.

1. Have PCS assets been recently inventoried (biannually or when a new item is procured), including applications, data, servers, workstations, field devices (e.g., programmable logic controllers), communications and network equipment? (ID.AM-1,ID.AM-2)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

2. Have business system assets been recently inventoried (biannually or when a new item is procured, including applications, data, servers, workstations, field devices (e.g., meter reading equipment), communications and network equipment? (ID.AM-1,ID.AM-2)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

3. Have the critical assets of the PCS been identified? (ID.AM-5,ID.BE-5)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

4. Have the risks and benefits of completely disconnecting the PCS from each network been evaluated? (ID.RA-5, DE.AE-4)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

5. Do you have an assigned information security officer? (ID.GV-2)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

6. Do you have a written cybersecurity policy for … (ID.GV-1)
   a. Process control systems?
      - ☐ Yes
      - ☐ No – Corrective Action:

        Target Completion Date:
      - ☐ N/A – Please Explain:

   b. Business enterprise systems?
      - ☐ Yes
      - ☐ No – Corrective Action:

        Target Completion Date:
      - ☐ N/A – Please Explain:

c. All levels of staff at the utility?
   ☐ Yes
   ☐ No – Corrective Action:

   Target Completion Date:
   ☐ N/A – Please Explain:

d. Outside entities (vendors, service providers, etc.)?
   ☐ Yes
   ☐ No – Corrective Action:

   Target Completion Date:
   ☐ N/A – Please Explain:

7. Are staff at all organizational levels and all outside entities periodically trained on … (PR.AT-1)
   a. The cyber security policy?
      ☐ Yes
      ☐ No – Corrective Action:

      Target Completion Date:
      ☐ N/A – Please Explain:

   b. Their cyber security roles and responsibilities?
      ☐ Yes
      ☐ No – Corrective Action:

      Target Completion Date:
      ☐ N/A – Please Explain:

   c. Cyber security threats?
      ☐ Yes
      ☐ No – Corrective Action:

      Target Completion Date:
      ☐ N/A – Please Explain:

8. Do you receive cyber security threat and vulnerability updates from information sharing entities such as US-CERT or WaterISAC? (ID.RA-2)
   ☐ Yes
   ☐ No – Corrective Action:

   Target Completion Date:
   ☐ N/A – Please Explain:

9. Are PCS assets physically secured from unauthorized personnel by….? (PR.AC-2)
    a. Electrical or mechanical door locks?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Guards or cameras?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Signs?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Barricades?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

10. Are business enterprise system assets physically secured from unauthorized personnel by….? (PR.AC-2)
    a. Electrical or mechanical door locks?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Guards or cameras?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

c. Signs?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

d. Barricades?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

11. Is there an updated access control list of all water system and non-water system personnel with access to the PCS? (PR.AC-1)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

12. Is there an updated access control list of all water system and non-water system personnel with access to the business enterprise system? (PR.AC-1)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

13. When personnel are no longer employed (whether terminated or resigned), or in a position where access is no longer needed, are their credentials within the systems terminated immediately? (PR.AC-1)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

14. Are PCS account privileges limited to only those privileges which are needed to complete required work? (PR.AC-4, PR.PT-3)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

15. Are business enterprise system account privileges limited to only those privileges which are needed to complete required work? (PR.AC-4, PR.PT-3)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

16. Is there a regularly updated list of all personnel with administrative privileges on the PCS? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

17. Is there a regularly updated list of all personnel with administrative privilegeson the business enterprise system? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

18. Are administrative privileges … (PR.AC-4, PR.AT-2)
    a. Limited only to dedicated administrator accounts?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Used only when carrying out administrative functions on the system?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

19. Are there restrictions on who can and cannot install software and updates? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

20. Have password policies been put in place which require… (PR.AC-1)
    a. Strong passwords (14 characters without multi-factor authentication (MFA) or 8 characters with MFA is recommended) which are changed regularly?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Each user to have unique credentials to log in to all PCS and business enterprise systems? (PR.AC-1)
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Different log in credentials for PCS and business enterprise systems?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Auto screen saver with password protection on all PCS? (PR.AC-1)
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    e. Auto screen saver with password protection on all business systems? (PR.AC-1)
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

21. Is a baseline of network operations and expected data flows for users and systems established and monitored? (DE.AE-1)
    ☐ Yes
    ☐ No – Corrective Action:

    Target Completion Date:
    ☐ N/A – Please Explain:

22. Is the network monitored to detect and alert on potential cyber security incidents? *(DE.CM-1)*
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

23. Is remote access for PCS via local area network, internet, or other means, protected by… (PR.AC-3, PR.AC-5)
    a. Firewall?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Password?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Dial back protocol or VPN?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    d. Multifactor authentication?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    e. Limiting permissions to only the minimum level required, e.g., using view-only webpages instead of allowing modification to system settings remotely?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

24. Is remote access for business systems via local area network, internet, or other means, protected by… (PR.AC-3, PR.AC-5)
    a. Firewall?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Password?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Dial back protocol or VPN?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Multifactor authentication?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    e. Limiting permissions to only the minimum level required, e.g., using view-only webpages instead of allowing modification to system settings remotely?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

25. Is encryption for PCS used for… (PR.DS-1, PR.DS-2, PR.PT-4)
    a. Data transfer?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

b. Data transfer on wireless links?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Stored data?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

26. Is encryption for business systems used for… (PR.DS-1, PR.DS-2, PR.PT-4)
    a. Data transfer?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Data transfer on wireless links?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Stored data?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

27. Are physically separate computer and network systems used for PCS and business enterprise functions? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

28. Do critical systems use application allowlisting, which only allows execution of approved files, applications, and programs? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

29. Has PCS equipment… (PR.AC-5, PR.PT-2)
    a. Been blocked from all non-PCS functions, including internet browsing and email access?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Been blocked from other non-PCS access to remote systems or services?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Had USB, DVD, and other external media ports disabled?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    d. Had auto-scan of removable media disabled?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

30. Are mobile devices (e.g., laptops, tablets, smartphones) which are used to access or control PCS equipment … (PR.AC-3)
    a. Included in established security policies?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

b. Encrypted?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Dedicated for PCS use only with non-essential software removed and any unnecessary functions disabled?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

31. Do PCS assets … (DE.CM-4, PR.IP-12)

a. Use anti-virus and anti-malware software?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

b. Regularly update virus and malware definitions?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Regularly scan storage media for viruses and malware?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

d. Install security patches on all systems regularly?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

32. Do the business enterprise systems … (DE.CM-4, PR.IP-12)
    a. Use anti-virus and anti-malware software?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Regularly update virus and malware definitions?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Regularly scan storage media for viruses and malware?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Install security patches on all systems regularly?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

33. For devices with memory capabilities (e.g., laptops, multi-function printers, and cell phones) are there policies in place for… (PR.DS-3, PR.IP-6)
    a. Transferring devices from one employee to another?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Removing or permanently destroying any stored data when removing devices from service?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

34. Is an uninterruptable power supply used for control continuance on PCS? (ID.BE-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

35. Are system and data backups performed regularly? (PR.IP-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

36. Has the system recently been successfully restored using backups (quarterly is recommended)? (PR.IP-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

37. Has a cyber security emergency response plan been established, and has it been reviewed in the past 12 months and updated when significant changes occur? (PR.IP-9)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

38. Have you had a cyber security audit of your system completed in the past 12 months?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

39. Do you regularly review your utility, local community, and other web sites for security sensitive information related to your system that could be used to disrupt your system or contaminate your water?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain: