PWS Name:
PWS #:

CYBERSECURITY VULNERABILITY ASSESSMENT

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.

Process control systems (PCS), such as SCADA systems, used to control plant treatment, monitoring or distributions functions at both local and remote facilities can, and have been targeted with malicious intent. Such attacks can cause significant harm by opening and closing valves, overriding alarms or disabling pumps or other equipment. Business systems used for accounts, billing and websites can also be targeted. Customer’s personal data can be stolen and systems can be compromised by malicious programs, such as ransomeware, disabling business or process control systems.

Connection of PCS or business systems to the internet or to local area networks (LANs) can create vulnerabilities. Remote access into PCS can also create potential vulnerability. Cyberattacks, however, are not limited only to internet based attacks. Physical security of all PCS and business systems to prevent unauthorized access to equipment is equally important.

The questions in the following checklist have been mapped back to components of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0). Industry and government collaborated to develop the *Framework*. It contains a number of 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.

The checklist has been compiled to assist with a basic cybersecurity assessment. It is not an exhaustive cyber security assessment and it may not be appropriate for all systems. Systems with large or complex cyber infrastructure may benefit from a more detailed cyber security assessment completed by an information technology or cyber security professional. You should consider the complexity of your system, the risk to your system and the potential impact to your system should a cyber attack occur, before deciding to use this tool.

Directions:
Answer each question. To answer some questions, you may need to consult with others, such as your information technology department, SCADA or PCS vendors, or other knowledgeable professionals. Each “No” answer should be investigated further as it may indicate a vulnerability to the system. Where vulnerabilities have been identified, appropriate mitigation measures should be proposed and a target completion date selected.

NEW YORK STATE | Department of Health

PWS Name:
PWS #:

Answers of “No” indicate a potential vulnerability which should be evaluated further.				
1	Have PCS and business system assets been recently inventoried, including applications, data, servers, workstations, field devices (e.g. programmable logic controllers), communications and network equipment? (ID.AM-1, ID.AM-2)	Yes □	No □	N/A □
2	Have the critical asset components of the PCS been identified? (ID.AM-5, ID.BE-5)	Yes □	No □	N/A □
3	Have the risks and benefits of completely disconnecting the PCS from all networks been evaluated? (ID.RA-5, DE.AE-4)	Yes □	No □	N/A □
4	Do you have an assigned information security officer? (ID.GV-2)	Yes □	No □	N/A □
5	Do you have a written cybersecurity policy for … (ID.GV-1)			
a	… PCS and business systems?	Yes □	No □	N/A □
b	… all levels of staff at the utility?	Yes □	No □	N/A □
c	… outside entities (vendors, service providers, etc.)?	Yes □	No □	N/A □
6	Are staff at all organizational levels and all outside entities periodically trained on … (PR.AT-1)			
a	… cyber security policy?	Yes □	No □	N/A □
b	… their cyber security roles and responsibilities?	Yes □	No □	N/A □
C	… cyber security threats?	Yes □	No □	N/A □
7	Do you receive cyber security threat and vulnerability updates from information sharing entities such as US-CERT or WaterISAC? (ID.RA-2)	Yes □	No □	N/A □
8	Are PCS and business system assets physically secured from unauthorized personnel? (PR.AC-2)	Yes □	No □	N/A □
9	Is there an updated Access Control List of all utility and non-utility personnel with access to the PCS or business system? (PR.AC-1)	Yes □	No □	N/A □
10	When personnel are no longer employed (whether terminated or resigned) are their credentials within the systems terminated immediately? (PR.AC-1)	Yes □	No □	N/A □
11	Are PCS and business system account privileges limited to only those privileges which are needed to complete required work? (PR.AC-4, PR.PT-3)	Yes □	No □	N/A □
12	Is there a regularly updated list of all personnel with administrative privileges on PCS or business system? (PR.AC-4)	Yes □	No □	N/A □
13	Are administrative privileges … (PR.AC-4, PR.AT-2)			
a	... limited only to accounts which require administrative privileges?	Yes □	No □	N/A □
b	… used only when carrying out administrative functions on the system?	Yes □	No □	N/A □

PWS Name:
PWS #:

14	Are there restrictions on who can/cannot install software and updates? (PR.AC-4)	Yes No N/A □ □ □
15	Have password policies been put in place which require… (PR.AC-1)	
a	… strong passwords which are changed regularly?	Yes No N/A □ □ □
b	… each user to have unique credentials to log in to all PCS and business systems? (PR.AC-1)	Yes No N/A □ □ □
c	… different log in credentials for PCS and business systems?	
d	… auto screen saver with password protection on all PCS and business systems? (PR.AC-1)	Yes No N/A □ □ □
16	Is a baseline of network operations and expected data flows for users and systems established and monitored? (DE.AE-1)	Yes No N/A □ □ □
17	Is the network monitored to detect and alert on potential cyber security events? (DE.CM-1)	Yes No N/A □ □ □
18	Is remote access via: local area network, internet, or other means, protected by… (PR.AC-3, PR.AC-5)	
a	… a firewall?	Yes No N/A □ □ □
b	… password?	Yes No N/A □ □ □
c	… dial back protocol?	Yes No N/A □ □ □
d	… secure token (Id card, S-Key, etc.)?	Yes No N/A □ □ □
e	… connection through a virtual private network (VPN)?	Yes No N/A □ □ □
f	… limited access to only the minimal level required (e.g. view-only web page)	Yes No N/A □ □ □
19	Is encryption used for… (PR.DS-1, PR.DS-2, PR.PT-4)	
a	… data transfer?	Yes No N/A □ □ □
b	… data transfer on wireless links?	Yes No N/A □ □ □
c	… stored data?	Yes No N/A □ □ □
20	Are physically separate computer and network systems used for PCS and business functions? (PR.AC-4)	Yes No N/A □ □ □
21	Do critical systems use application whitelisting, which allows execution of approved files, applications and programs only? (PR.AC-4)	Yes No N/A □ □ □
22	Has PCS equipment… (PR.AC-5, PR.PT-2)	Yes No N/A □ □ □
a	… been blocked from all non-PCS functions, including internet browsing and email access?	Yes No N/A □ □ □

PWS Name:
PWS #:

b	… been blocked from other non-PCS access to remote systems or services?	Yes No N/A □ □ □
c	… had USB, DVD, and other external media ports disabled?	Yes No N/A □ □ □
d	… had auto-scan of removable media disabled?	Yes No N/A □ □ □
23	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 N/A □ □ □
b	… encrypted?	Yes No N/A □ □ □
c	… dedicated for PCS use only with non-essential software removed and any unnecessary functions disabled?	Yes No N/A □ □ □
24	Do the PCS and business systems … (DE.CM-4, PR.IP-12)	
a	… use anti-virus and anti-malware software?	Yes No N/A □ □ □
b	… regularly update virus and malware definitions?	Yes No N/A □ □ □
c	… regularly scan storage media for viruses and malware?	Yes No N/A □ □ □
d	… install security patches on all systems regularly?	Yes No N/A □ □ □
25	For devices with memory capabilities (e.g. laptops, multi-function printers, cell phones, etc.) are there policies in place for… (PR.DS-3, PR.IP-6)	
a	… transferring devices from one employee to another?	Yes No N/A □ □ □
b	… removing or permanently destroying any stored data when removing devices from service?	Yes No N/A □ □ □
26	Is an uninterruptable power supply used for continuance control? (ID.BE-4)	Yes No N/A □ □ □
27	Are system and data backups performed regularly? (PR.IP-4)	Yes No N/A □ □ □
28	Has the system recently been successfully restored using backups? (PR.IP-4)	Yes No N/A □ □ □
29	Has a cyber security emergency response plan been established, and has is it been reviewed and updated recently? (PR.IP-9)	Yes No N/A □ □ □
30	Have you had a recent cyber security audit of your system completed?	Yes No N/A □ □ □

PWS Name:
PWS #:

Enter identified vulnerabilities in the table below. Propose actions to remove or reduce the risk and include a target date for completion. Use additional pages if needed.

Question Number	Anticipated Corrective Action	Priority	Target Completion Date

H = Highest Priority   M = Medium Priority   L = Lower Priority

PWS Name:
PWS #:

Question Number	Anticipated Corrective Action	Priority	Target Completion Date