Water Sector Cybersecurity Evaluation Program

April 26, 2023

United States Environmental Protection Agency

Office of Water

Presenter

Brandon M. Carter

Sr. Cybersecurity Specialist

U.S. EPA - Office of Water

Agenda

- **Summary of EPA Memorandum- “Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process”**

- **Overview of the Cybersecurity Evaluation Program**

Summary of New EPA Memorandum "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process"

Memo Overview

- **The memo interprets existing regulations to require state oversight of cybersecurity practices at PWSs. States must evaluate the cybersecurity of operational technology OT used by a PWS when conducting periodic audits of PWSs, called sanitary surveys, or through other state programs.**

- **If the PWS uses an ICS or other OT as part of the equipment or operation of any required component of the sanitary survey, then the state must evaluate the adequacy of the cybersecurity of that OT for producing and distributing safe drinking water.**

- **If the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency.**

Flexible Approaches to Include Cybersecurity in PWS Sanitary Surveys

- **Option 1:** **Self-assessment or third-party assessment of cybersecurity practices - 1b. EPA's Water Sector Cybersecurity Evaluation Program**

- **Option 2:** **State evaluation of cybersecurity practices during the sanitary survey – EPA Direct Implementation Programs: EPA's Water Sector Cybersecurity Evaluation Program**

- **Option 3:** **Alternate state program for water system cybersecurity evaluation**

Self-Assessment or Third-Party Assessment

Option 1.a – Self Assessment

- **PWSs conduct the cybersecurity assessment themselves using EPA's optional method or another government or private-sector method.**

Option 1.b – Third-Party Assessment

- **PWS undergoes an assessment of cybersecurity practices by an outside party, such as EPA's Water Sector Cybersecurity Evaluation Program, or another government or private sector technical assistance provider approved by the state.**

Option 1: Self-Assessment or Third-Party Assessment of Cybersecurity Practices

- **Under Options 1.a and 1.b, the cybersecurity self or third-party assessment should be completed prior to the sanitary survey, made available to state sanitary surveyors, and then updated to reflect changes in cybersecurity practices and/or OT prior to subsequent sanitary surveys.**
- **During the sanitary survey, the state surveyor should confirm completion of the assessment and determine whether identified cybersecurity gaps are significant deficiencies.**

Implementation Options

Additional Information:

- **Primacy agencies will choose their option over the coming months. PWSs should consult directly with them to confirm the chosen option.**
- **PWSs are encouraged to start assessing your cybersecurity posture as soon as possible, irrespective of the state's chosen option.**

Overview of
EPA Water Sector Cybersecurity Evaluation Program

EPA Water Sector Cybersecurity Evaluation Program

- **Free assessment of cybersecurity gaps or vulnerabilities in the OT used by public water systems (PWSs).**

- **During the assessment, the EPA contractor will ask the PWS each of the questions in the EPA Checklist**

Account Security. *Does the PWS...*

1.1. Detect and block repeated unsuccessful login attempts?

Recommendation: Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.

1.2. Change default passwords?

Recommendation: When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.

1.3. Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?

Recommendation: Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.

1.4. Require a minimum length for passwords?

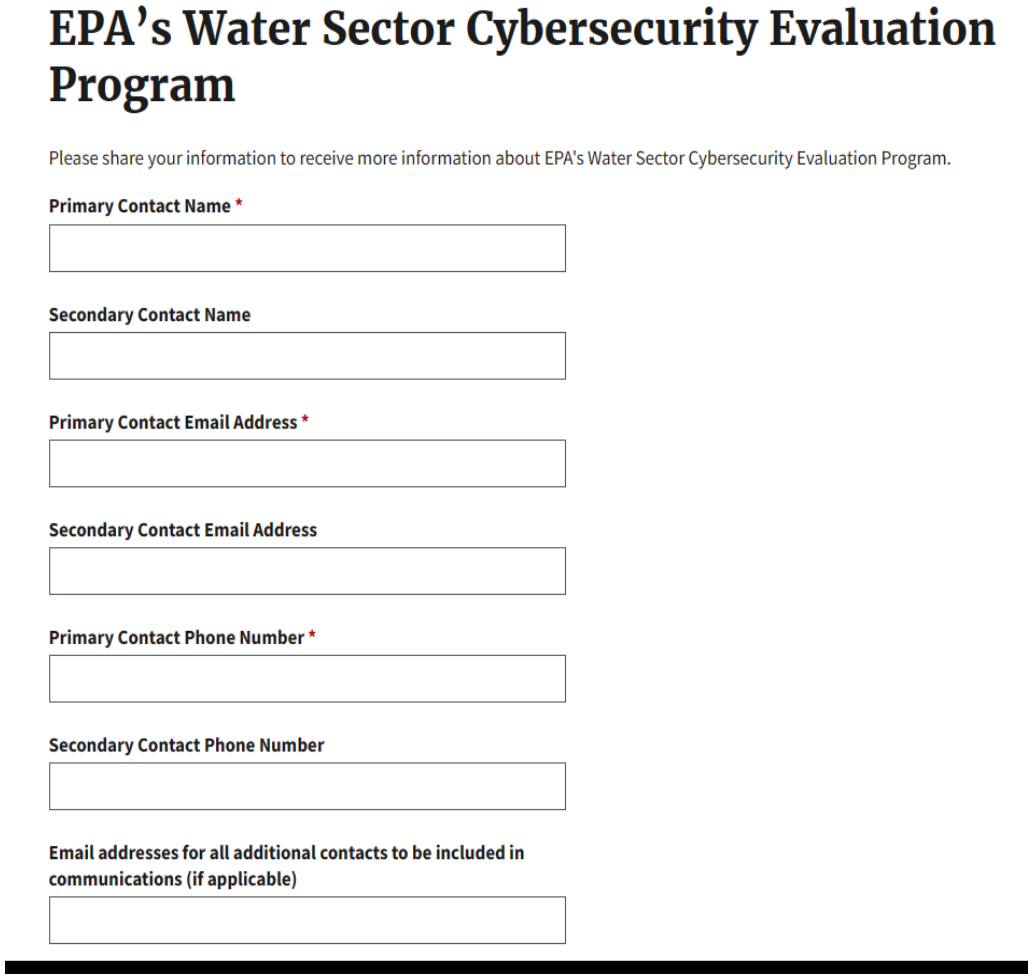
Recommendation: Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.

1.5. Separate user and privileged (e.g., System Administrator) accounts?

Recommendation: Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.

How do I register?

- **When a PWS registers to participate in this program, an EPA contractor will contact the PWS schedule the assessment.**
  - https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program
- **Timeline:**
  - Establishing contact with the PWS after Registration: **within 1 business day**
  - Scheduling the Assessment: **3 to 5 business days (after initial contact with PWS)**
  - Conducting the Assessment: **45 to 90 minutes**
  - Date that the PWS will received the assessment report: **within one business day (following completion of the assessment)**



EPA's Water Sector Cybersecurity Evaluation Program

Please share your information to receive more information about EPA's Water Sector Cybersecurity Evaluation Program.

Primary Contact Name *

Secondary Contact Name

Primary Contact Email Address *

Secondary Contact Email Address

Primary Contact Phone Number *

Secondary Contact Phone Number

Email addresses for all additional contacts to be included in communications (if applicable)

What does the PWS need to prepare before the assessment?

- **Utilities will need to gather:**
  - input from management, operations, business, and OT and information technology (IT) staff as appropriate
  - existing system documentation, diagrams, policies, and procedures to help answer the checklist questions

Gather Appropriate Staff

- **Planning and conducting a cybersecurity assessment should be a group effort among PWS staff. It will be helpful to gather in a setting such as a conference room.**

Suggested PWS Staff to Participate in the Cybersecurity Self-Assessment
Named role/position/title that is responsible for all PWS cybersecurity activities
Cybersecurity Staff
Managers
OT and IT Staff
Operators

Collect Existing Supporting Cybersecurity Documentation

- **If the PWS has existing supporting cybersecurity documentation, this will be helpful during the cybersecurity assessment. Additionally, a PWS may need to provide supporting documentation surveyors during the sanitary survey.**

Examples of Supporting Cybersecurity Documentation:
Cybersecurity Policies and Procedures
Emergency and Incident Response Plans that include Cybersecurity
Vendor Lists and Relevant Information
Cybersecurity Program Documentation
Software Licenses and Packages
Inventories of all IT and OT Devices
Network Drawings and Diagrams

What assessment does the evaluation use?

- **EPA Cybersecurity Checklist for Public Water System Sanitary Surveys**
  - Provides a method to evaluate cybersecurity at a PWS during a sanitary survey.
  - Derived directly from CISA's 2022 Cross-Sector Cybersecurity Performance Goals.
  - Written in a simplified question format to facilitate their use in evaluating cybersecurity at a PWS.

Account Security. *Does the PWS...*

1.1. Detect and block repeated unsuccessful login attempts?

Recommendation: Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.

1.2. Change default passwords?

Recommendation: When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.

1.3. Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?

Recommendation: Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.

1.4. Require a minimum length for passwords?

Recommendation: Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.

1.5. Separate user and privileged (e.g., System Administrator) accounts?

Recommendation: Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.

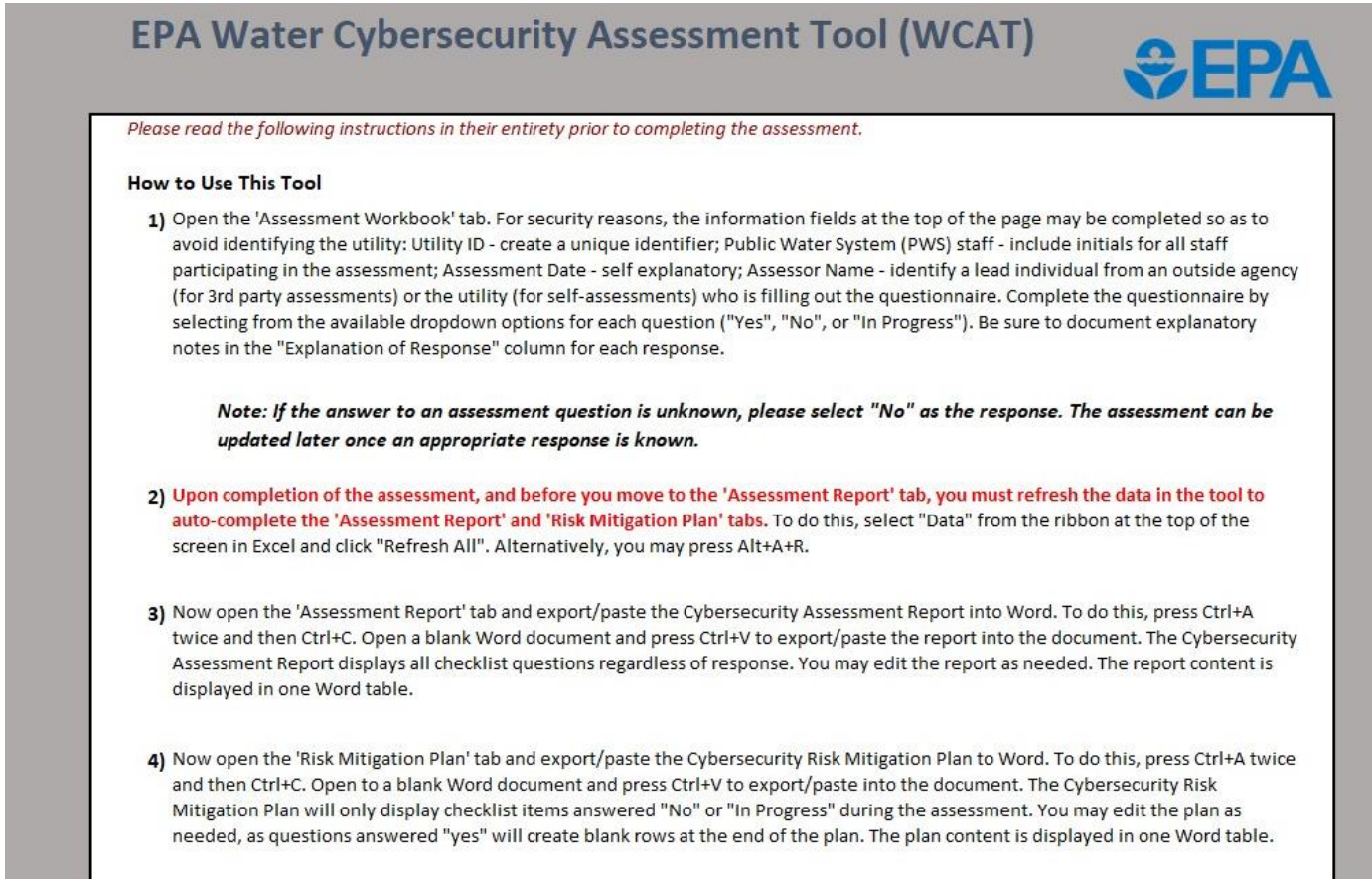
Overview of EPA's Cybersecurity Checklist for Public Water System Sanitary Surveys

Cybersecurity Control Family	# of Questions/Goals
1. Account Security	7
2. Device Security	5
3. Data Security	4
4. Governance and Training	5
5. Vulnerability Management	3
6. Supply Chain/Third Party	2
7. Response and Recovery	4
8. Other	3
Total:	33

EPA Water Cybersecurity Assessment Tool (WCAT)

- **Provides a method to evaluate cybersecurity at a PWS during a sanitary survey.**

- **Includes tabs for:**
  - Assessment Workbook
  - Assessment Report
  - Risk Mitigation Plan



EPA Water Cybersecurity Assessment Tool (WCAT)

Please read the following instructions in their entirety prior to completing the assessment.

How to Use This Tool

1) Open the 'Assessment Workbook' tab. For security reasons, the information fields at the top of the page may be completed so as to avoid identifying the utility: Utility ID - create a unique identifier; Public Water System (PWS) staff - include initials for all staff participating in the assessment; Assessment Date - self explanatory; Assessor Name - identify a lead individual from an outside agency (for 3rd party assessments) or the utility (for self-assessments) who is filling out the questionnaire. Complete the questionnaire by selecting from the available dropdown options for each question ("Yes", "No", or "In Progress"). Be sure to document explanatory notes in the "Explanation of Response" column for each response.

Note: If the answer to an assessment question is unknown, please select "No" as the response. The assessment can be updated later once an appropriate response is known.

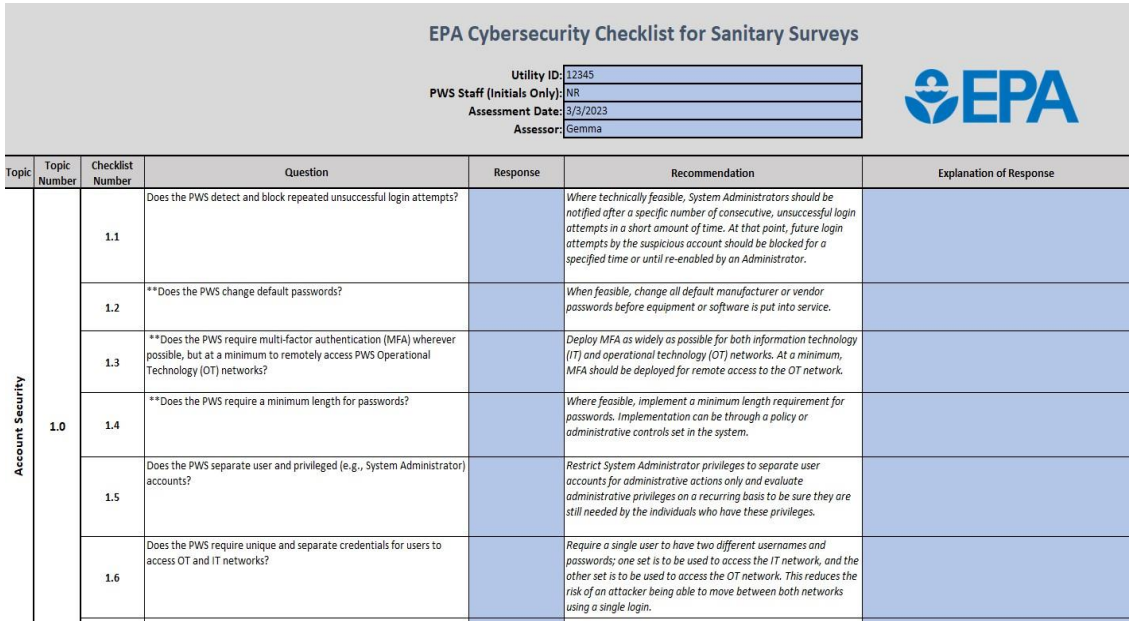
2) **Upon completion of the assessment, and before you move to the 'Assessment Report' tab, you must refresh the data in the tool to auto-complete the 'Assessment Report' and 'Risk Mitigation Plan' tabs.** To do this, select "Data" from the ribbon at the top of the screen in Excel and click "Refresh All". Alternatively, you may press Alt+A+R.

3) Now open the 'Assessment Report' tab and export/paste the Cybersecurity Assessment Report into Word. To do this, press Ctrl+A twice and then Ctrl+C. Open a blank Word document and press Ctrl+V to export/paste the report into the document. The Cybersecurity Assessment Report displays all checklist questions regardless of response. You may edit the report as needed. The report content is displayed in one Word table.

4) Now open the 'Risk Mitigation Plan' tab and export/paste the Cybersecurity Risk Mitigation Plan to Word. To do this, press Ctrl+A twice and then Ctrl+C. Open to a blank Word document and press Ctrl+V to export/paste into the document. The Cybersecurity Risk Mitigation Plan will only display checklist items answered "No" or "In Progress" during the assessment. You may edit the plan as needed, as questions answered "yes" will create blank rows at the end of the plan. The plan content is displayed in one Word table.

What is the evaluation process?

- **Your responses to these questions will generate what will be included in the assessment**
- **There are three responses to each question**
  - Yes
  - No
  - In Progress
- **Each response will be accompanied by an "*explanation of response*"**
- **The responses to the checklist will generate a report that identifies potential cybersecurity gaps or vulnerabilities in the PWS's OT**



EPA Cybersecurity Checklist for Sanitary Surveys

Utility ID: 12345
PWS Staff (Initials Only): NR
Assessment Date: 3/3/2023
Assessor: Gemma

Topic	Topic Number	Checklist Number	Question	Response	Recommendation	Explanation of Response
Account Security	1.0	1.1	Does the PWS detect and block repeated unsuccessful login attempts?		*Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.*	
		1.2	**Does the PWS change default passwords?		*When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.*	
		1.3	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?		*Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.*	
		1.4	**Does the PWS require a minimum length for passwords?		*Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.*	
		1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?		*Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.*	
		1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?		*Require a single user to have two different usernames and passwords; one set is to be used to access the IT network, and the other set is to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.*	

Assessment Workbook

EPA Cybersecurity Checklist for Sanitary Surveys

Utility ID:	12345
PWS Staff (Initials Only):	NR
Assessment Date:	3/3/2023
Assessor:	Gemma

Topic	Topic Number	Checklist Number	Question	Response	Recommendation	Explanation of Response
Account Security	1.0	1.1	Does the PWS detect and block repeated unsuccessful login attempts?		*Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.*	
		1.2	**Does the PWS change default passwords?		*When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.*	
		1.3	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?		*Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.*	
		1.4	**Does the PWS require a minimum length for passwords?		*Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.*	
		1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?		*Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.*	
		1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?		*Require a single user to have two different usernames and passwords; one set is to be used to access the IT network, and the other set is to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.*	

HOW DO UTILITIES USE THESE: EPA Cybersecurity Checklist Fact Sheets

- **Fact Sheets are available for each question on the EPA Checklist and include additional information including:**
  - Recommendations
  - Overview of why the control is important
  - Additional Guidance
  - Implementation Tips
  - Additional Resources
  - Estimate for Cost, Impact, and Complexity

Account Security: Detection of Unsuccessful (Automated) Login Attempts

COST: $$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

1.1: Does the PWS detect and block repeated unsuccessful login attempts?

Recommendation: Where technically feasible, system administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an administrator.

Why is this control important?

A common technique that attackers use to break into OT and IT systems is to attempt to "guess" an actual username and password login combination. This can be accomplished by manually guessing an account's password, using a list of common passwords, or through a technique called a *brute force attack*. In this type of attack, an attacker uses a trial-and-error approach to systematically guess login credentials. The attacker submits combinations of usernames and passwords, generally using an automated password-breaking tool, until the guess is correct. Blocking an attacker from future guesses after a specified number of incorrect guesses can stop these types of attacks.

Additional Guidance

- Enable systems to automatically notify (e.g., by a computer-generated alert) security teams or the system administrator after a specific number of consecutive, unsuccessful login attempts in a short time period (e.g., five failed attempts in under 2 minutes).
- Enable account lockout settings on applicable systems to prevent future login attempts for the suspicious account for a minimum time or until the account is re-enabled by the system administrator.
- It is a good practice to ensure that the account lockout duration is set to 15 minutes (or more) or to require a user with administrative privileges to unlock a user's account.
- Log and store the alert information for analysis. Use sound logging procedures - a log should capture event source, date, username, timestamp, source addresses, destination addresses, and any other useful information that could assist in a forensic investigation.

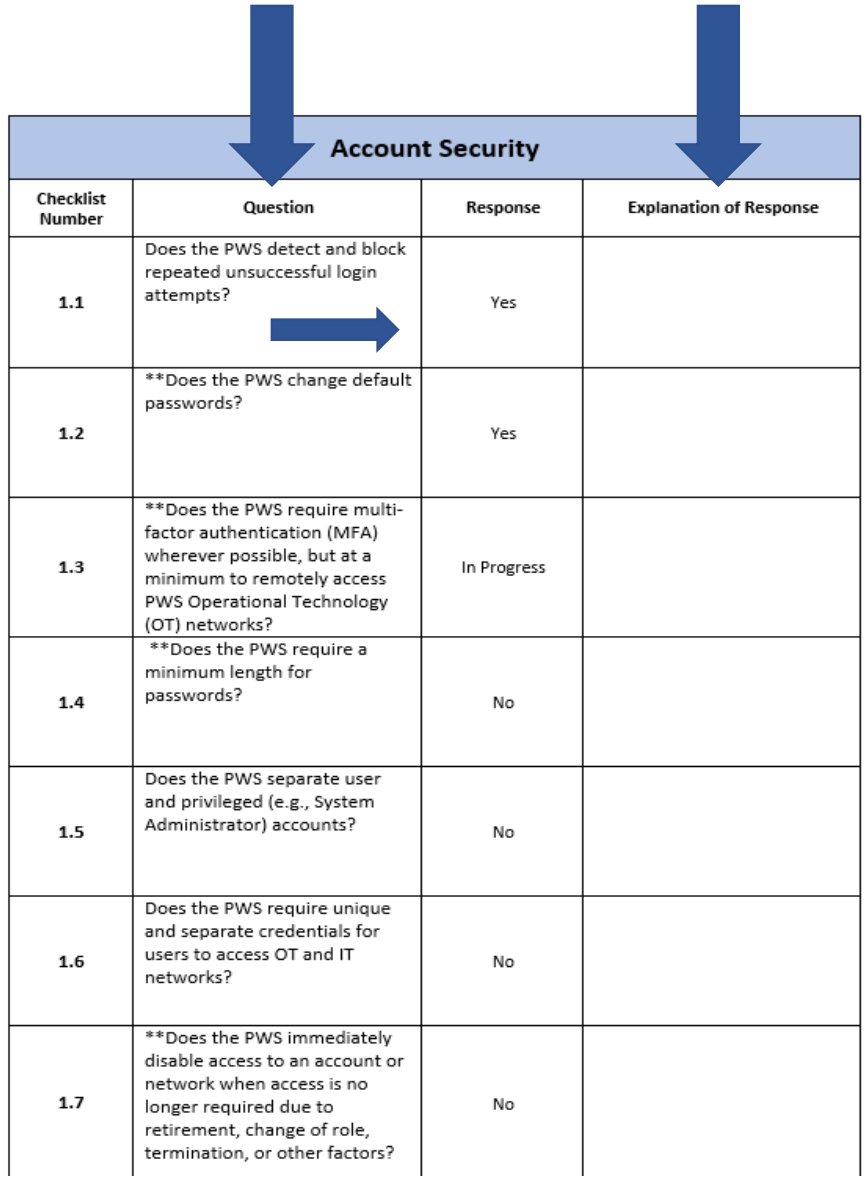
Implementation Tips

Depending on your version of Windows, you can use the Local Security Policy to restrict the number of login attempts. To access this feature, type "Local Security Policy" in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on "Account Policies" to adjust login attempts and lockout duration.

If your PWS utilizes a Microsoft Domain where many systems and user accounts are connected to a single domain, these settings can be managed using Group Policy Objects (GPOs). The Account Lockout Policy settings can be enabled in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security

Assessment Report Tab

- **Provides a summary of results from the completed Cybersecurity Assessment.**
- **Report can be shared with state surveyor during Sanitary Survey.**
- **Questions indicated with double asterisks (**) represent EPA suggested significant deficiencies.**



Account Security			
Checklist Number	Question	Response	Explanation of Response
1.1	Does the PWS detect and block repeated unsuccessful login attempts?	Yes	
1.2	**Does the PWS change default passwords?	Yes	
1.3	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?	In Progress	
1.4	**Does the PWS require a minimum length for passwords?	No	
1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?	No	
1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?	No	
1.7	**Does the PWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?	No	

Risk Mitigation Plan

- **The Risk Mitigation Plan documents the actions the PWS is taking or intends to take to address cybersecurity risks.**
- **The actions in this plan are responsive to the cybersecurity assessment conducted using the EPA Cybersecurity Checklist for Public Water System Sanitary Surveys.**
- **The Risk Mitigation Plan includes all questions from the EPA Checklist where PWS representatives responded either "No" or "In Progress" during the assessment.**

Account Security	1.3	Question:	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?
		Planned Risk Mitigation Action:	*Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.*
		Current Status:	
		Target Completion Date:	
		PWS Personnel Responsible:	
		Involved Departments and/or Agencies:	
		PWS Notes:	
Account Security	1.4	Question:	**Does the PWS require a minimum length for passwords?
		Planned Risk Mitigation Action:	*Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.*
		Current Status:	
		Target Completion Date:	
		PWS Personnel Responsible:	
		Involved Departments and/or Agencies:	
		PWS Notes:	

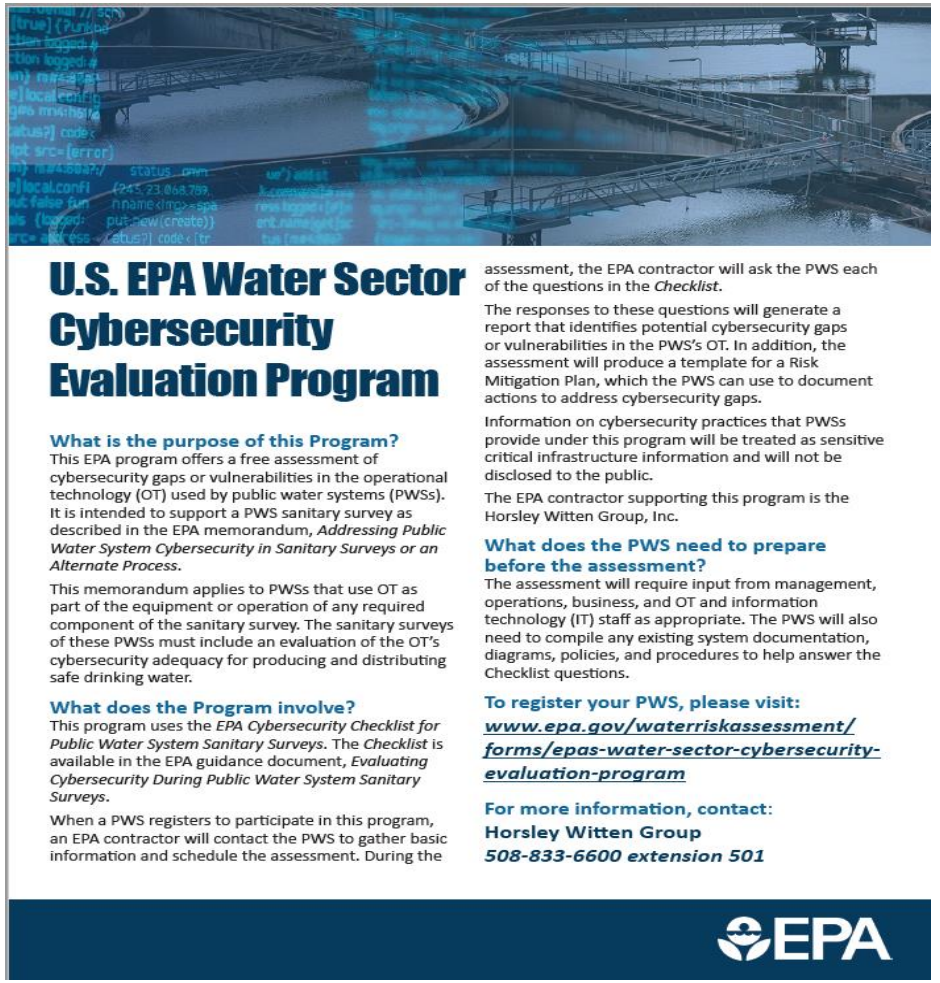
EPA Water Sector Cybersecurity Evaluation Program

- **PWSs will receive a report with response to the checklist questions that shows cybersecurity gaps.**
- **PWS must have the evaluation prior to the sanitary survey**
- **The PWS will provide the assessment report to the state to review during the sanitary survey.**

SAMPLE REPORT

For More Information on the Cybersecurity Evaluation Program

- **Contact Horsley Witten Group: 508-833-6600 extension 501**



U.S. EPA Water Sector Cybersecurity Evaluation Program

What is the purpose of this Program?
This EPA program offers a free assessment of cybersecurity gaps or vulnerabilities in the operational technology (OT) used by public water systems (PWSs). It is intended to support a PWS sanitary survey as described in the EPA memorandum, *Addressing Public Water System Cybersecurity in Sanitary Surveys or an Alternate Process*.

This memorandum applies to PWSs that use OT as part of the equipment or operation of any required component of the sanitary survey. The sanitary surveys of these PWSs must include an evaluation of the OT's cybersecurity adequacy for producing and distributing safe drinking water.

What does the Program involve?
This program uses the *EPA Cybersecurity Checklist for Public Water System Sanitary Surveys*. The *Checklist* is available in the EPA guidance document, *Evaluating Cybersecurity During Public Water System Sanitary Surveys*.

When a PWS registers to participate in this program, an EPA contractor will contact the PWS to gather basic information and schedule the assessment. During the assessment, the EPA contractor will ask the PWS each of the questions in the *Checklist*.

The responses to these questions will generate a report that identifies potential cybersecurity gaps or vulnerabilities in the PWS's OT. In addition, the assessment will produce a template for a Risk Mitigation Plan, which the PWS can use to document actions to address cybersecurity gaps.

Information on cybersecurity practices that PWSs provide under this program will be treated as sensitive critical infrastructure information and will not be disclosed to the public.

The EPA contractor supporting this program is the Horsley Witten Group, Inc.

What does the PWS need to prepare before the assessment?
The assessment will require input from management, operations, business, and OT and information technology (IT) staff as appropriate. The PWS will also need to compile any existing system documentation, diagrams, policies, and procedures to help answer the Checklist questions.

To register your PWS, please visit:
www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program

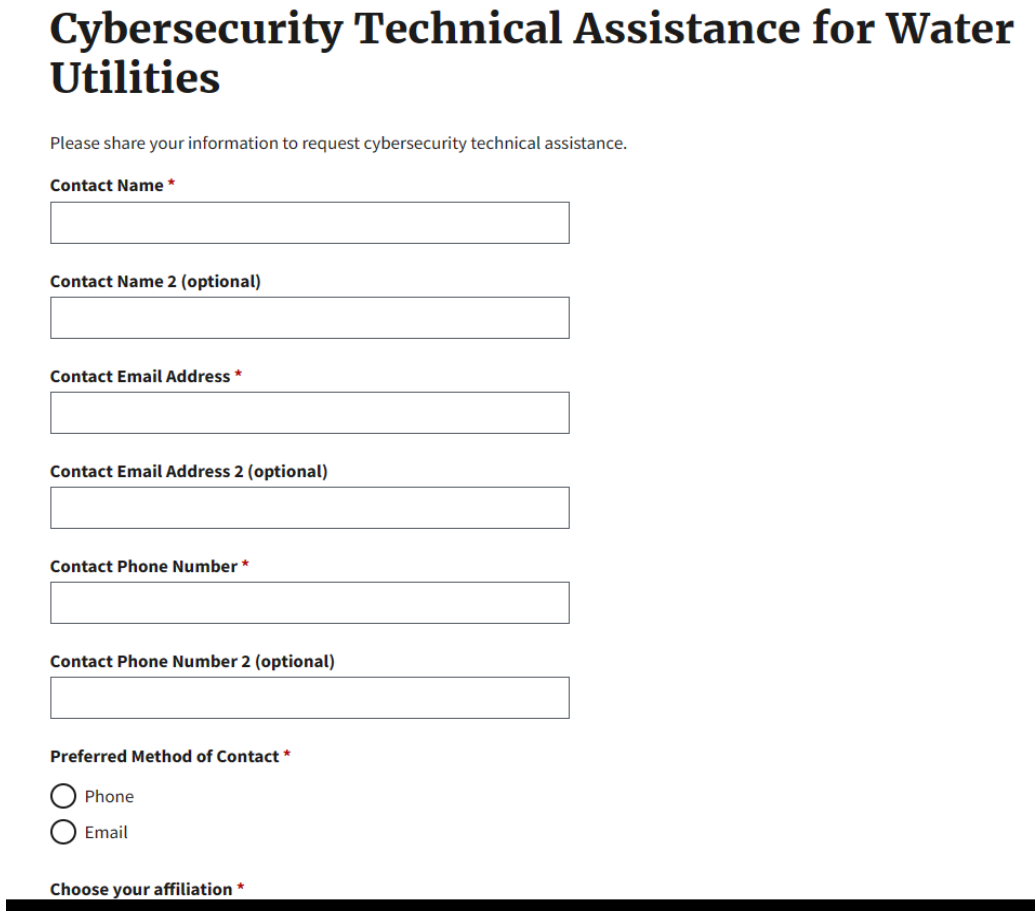
For more information, contact:
Horsley Witten Group
508-833-6600 extension 501

EPA

Overview of Cybersecurity Technical Assistance Program for the Water Sector

Cybersecurity Technical Assistance Program for the Water Sector

- **Under this program, states and PWSs can submit questions or request to consult with a subject matter expert (SME) regarding cybersecurity in sanitary surveys.**
- **EPA will strive to have an SME respond within two business days.**
- **All assistance will be remote.**
- **Link: https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities**



Cybersecurity Technical Assistance for Water Utilities

Please share your information to request cybersecurity technical assistance.

Contact Name *

Contact Name 2 (optional)

Contact Email Address *

Contact Email Address 2 (optional)

Contact Phone Number *

Contact Phone Number 2 (optional)

Preferred Method of Contact *

Phone

Email

Choose your affiliation *

Link to EPA's Website

https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector