Overview of EPA’s Memorandum:

“Addressing PWS cybersecurity in sanitary surveys or an alternate process”

4/12/23

EPA United States Environmental Protection Agency

Office of Water

Agenda

- Memorandum Overview
- Guidance and Resources
- Training

Memorandum’s Purpose

“To express EPA’s commitment in partnering with co-regulators in states to ensure that all PWSs employ essential best practices for cybersecurity to protect public health”

Note: “state” in this memo and training means the definition in 40 Code of Federal Regulations (CFR) § 141.2, which is “the agency of the State [including territories] or Tribal government which has jurisdiction over public water systems”

Why is EPA taking this action?

- Cyber-attacks against critical infrastructure facilities, including public water systems (PWSs), are increasing
- Past incidents have shown these attacks have the potential to disable or contaminate the delivery of drinking water to consumers and other essential facilities
- While some PWSs have taken steps to improve cybersecurity, recent events show many PWSs have failed to adopt basic cybersecurity best practices

What is EPA Interpreting?

EPA interprets the regulatory requirements relating to the conduct of a sanitary survey to require that when a PWS uses operational technology (OT), such as an industrial control system (ICS), as part of the equipment or operation of any required component of a sanitary survey, then the sanitary survey must include an evaluation of the adequacy of the cybersecurity of that OT for producing and distributing safe drinking water.

The interpretation clarifies that the regulatory requirement to review the "equipment" and "operation" of a PWS must encompass a review of the cybersecurity practices and controls needed to maintain the integrity and continued functioning of OT of the PWS that could impact the supply or safety of the water provided to customers.

State Role

During a sanitary survey of a PWS, states must do the following to comply with the federal definition of “sanitary survey”:

(1) 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, including the cybersecurity of interdependent systems, for producing and distributing safe drinking water

(2) 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

Cybersecurity Significant Deficiencies

Should include the absence of a practice or control, or the presence of a vulnerability, that has a high risk of being exploited either directly or indirectly, to compromise an OT used in the treatment or distribution of drinking water

Note: States retain their existing legal flexibility with sanitary surveys in how they evaluate PWSs, identify significant deficiencies, and require PWSs to address significant deficiencies

Which PWSs do not require a cybersecurity evaluation during a sanitary survey?

When a PWS does not use OT, such as a Supervisory Control and Data Acquisition (SCADA) system, ICS, or networked programmable logic controllers (PLCs), as part of the equipment or operation of any required component of a sanitary survey, then the PWS sanitary survey is not required to include an evaluation of cybersecurity

What does this mean for your programs? You will need to identify the systems that do and do not require a cyber evaluation.

Flexible Approaches to Include Cybersecurity in PWS Sanitary Surveys

- **Option 1:** Self-assessment or third-party assessment of cybersecurity practices
- **Option 2:** State evaluation of cybersecurity practices during the sanitary survey
- **Option 3:** Alternate State Program for Water System Cybersecurity Evaluation

Option 1: Self-assessment or third-party assessment of cybersecurity practices

- States that ***have or establish the requisite authority*** may require PWSs to conduct a self-assessment of cybersecurity practices for the purpose of identifying Cybersecurity Gaps

- Cybersecurity Gaps are the absence of recommended cybersecurity practices or controls, or the presence of vulnerabilities

- Option 1 has two subsets, Option 1.a Self Assessment and Option 1.b Third-Party Assessment

Self-Assessment or Third-Party Assessment

Option 1.a – PWS Self Assessment

- PWSs conduct the cybersecurity assessment themselves using EPA's Checklist 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 operational technology 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

Option 1: Self-assessment or third-party assessment of cybersecurity practices

- States may require PWSs to develop follow-on risk mitigation plans to address cybersecurity gaps identified during the assessment, specifically including any significant deficiencies if designated by the state

- The risk mitigation plan would list planned mitigation actions and schedules. The state would review the risk mitigation plan during the sanitary survey, ensure the PWS is taking necessary steps to address any significant deficiencies, and offer to identify additional resources PWSs could use to address those gaps

Option 2: State evaluation of cybersecurity practices during the sanitary survey

- Surveyors will evaluate cybersecurity practices directly during a sanitary survey of a PWS to identify cybersecurity gaps and determine if any of those gaps should be designated as significant deficiencies

- This approach is consistent with how states conduct sanitary surveys of other components of PWS operations

Option 2: State evaluation of cybersecurity practices during the sanitary survey

- The state, rather than the PWS or a third party, would conduct the cybersecurity assessment and direct the PWS to address any significant deficiencies that the state identifies

- EPA is providing training and technical assistance on evaluating cybersecurity in PWS sanitary surveys to assist states that take this approach

Option 3: Alternative State Program for Water System Cybersecurity

- Several states have programs under which PWSs assess cybersecurity gaps (which may be called “security gaps,” “vulnerabilities,” or their equivalent) in their current practices that could impact safe drinking water and implement controls to address those gaps

- States that currently have or that develop such a program may use this program as an alternative to including cybersecurity in PWS sanitary surveys

Examples of Alternative State Programs

- A state homeland security agency may have a cybersecurity program covering all critical infrastructure in the state

- A state emergency management agency that conducts the cybersecurity assessment for the PWS instead of, or in collaboration with, the state agency responsible for the PWS supervision program

Option 3: Alternative State Program for Water System Cybersecurity

- PWSs serving Rural Communities with populations of less than 10,000 can utilize US Department of Agriculture (USDA) Rural Development (RD) funded technical assistance providers

- These communities may also already have requirements to complete cybersecurity analysis as part of loan and grant terms with USDA RD

Option 3: Alternative State Program for Water System Cybersecurity

- To be at least as stringent as a sanitary survey, state surveyors must ensure that the alternate state programs effectively identify cybersecurity gaps (or equivalent) through an assessment and that the PWSs address any significant deficiencies if designated by the state
- Further, the cybersecurity assessment must be conducted at least as often as the required sanitary survey frequency for the PWS (typically 3 or 5 years)

EPA Guidance and Resources

United States
Environmental Protection
Agency

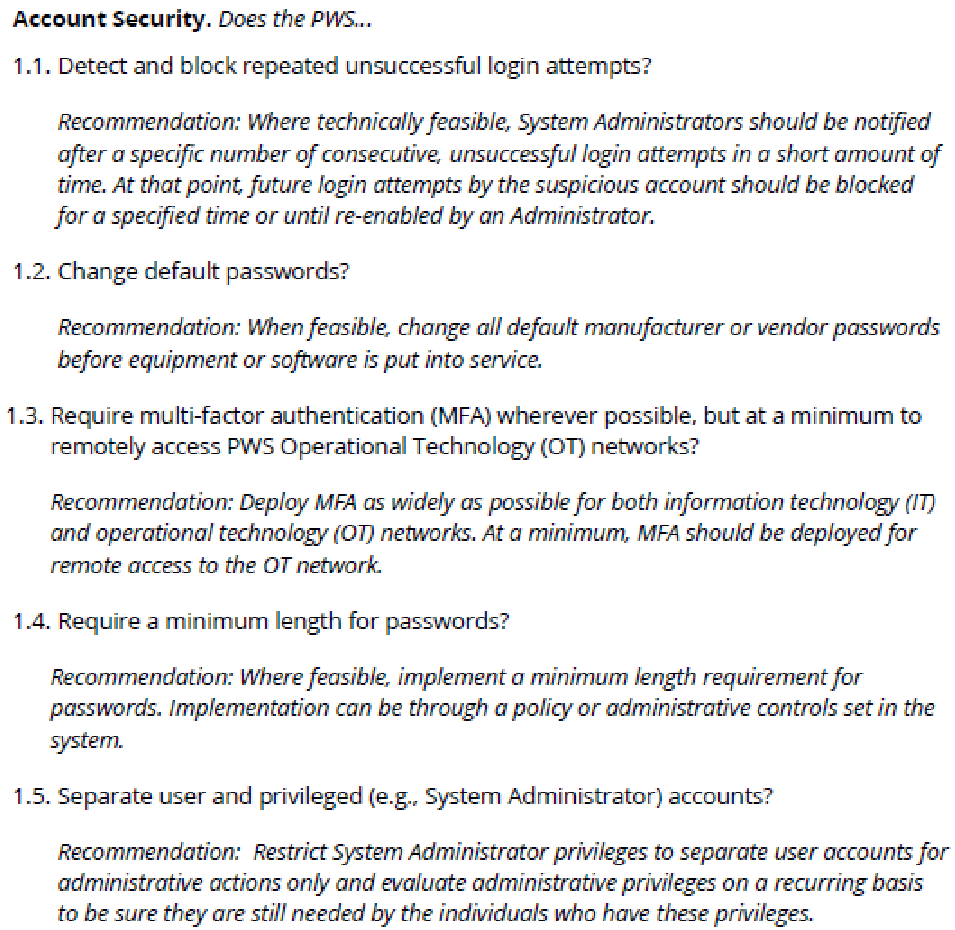
Office of Water

Evaluating Cybersecurity During Public Water System Sanitary Survey

- This guidance document includes information on the following to support evaluating cybersecurity in PWS sanitary surveys:
  - EPA Cybersecurity Checklist for Public Water System Sanitary Surveys
  - EPA Checklist Fact Sheets
  - Potential Significant Deficiencies

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.

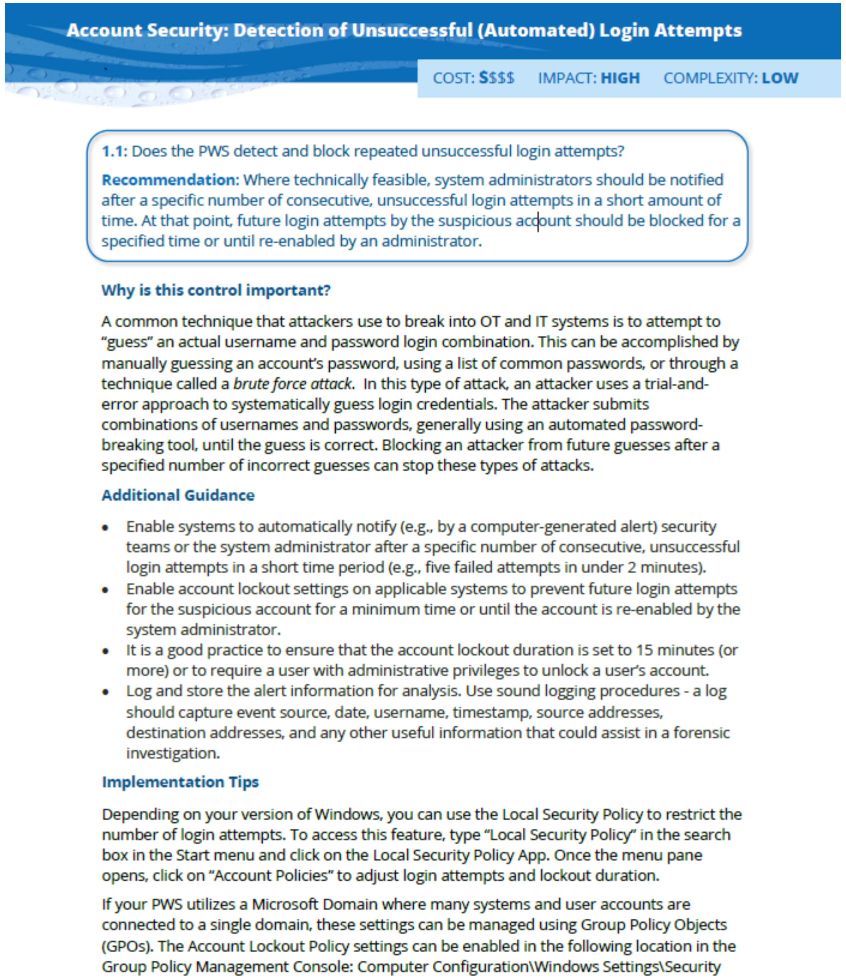
1.5. Separate user and privileged (e.g., System Administrator) accounts?

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.

EPA Cybersecurity Checklist Fact Sheets

Fact Sheets are available for each question on the EPA Checklist and include additional information including:

1. Recommendations
2. Overview of why the control is important
3. Additional Guidance
4. Implementation Tips
5. Additional Resources
6. 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

Potential Significant Deficiencies

- EPA considered the following factors when identifying potential significant deficiencies:

➢ High Risk and history of exploitation in the water sector or other critical infrastructures
➢ Technically feasible for most PWSs to address
➢ Significant capital expenditures are not typically required
➢ Near-term implementation timeframe (usually less than one year)

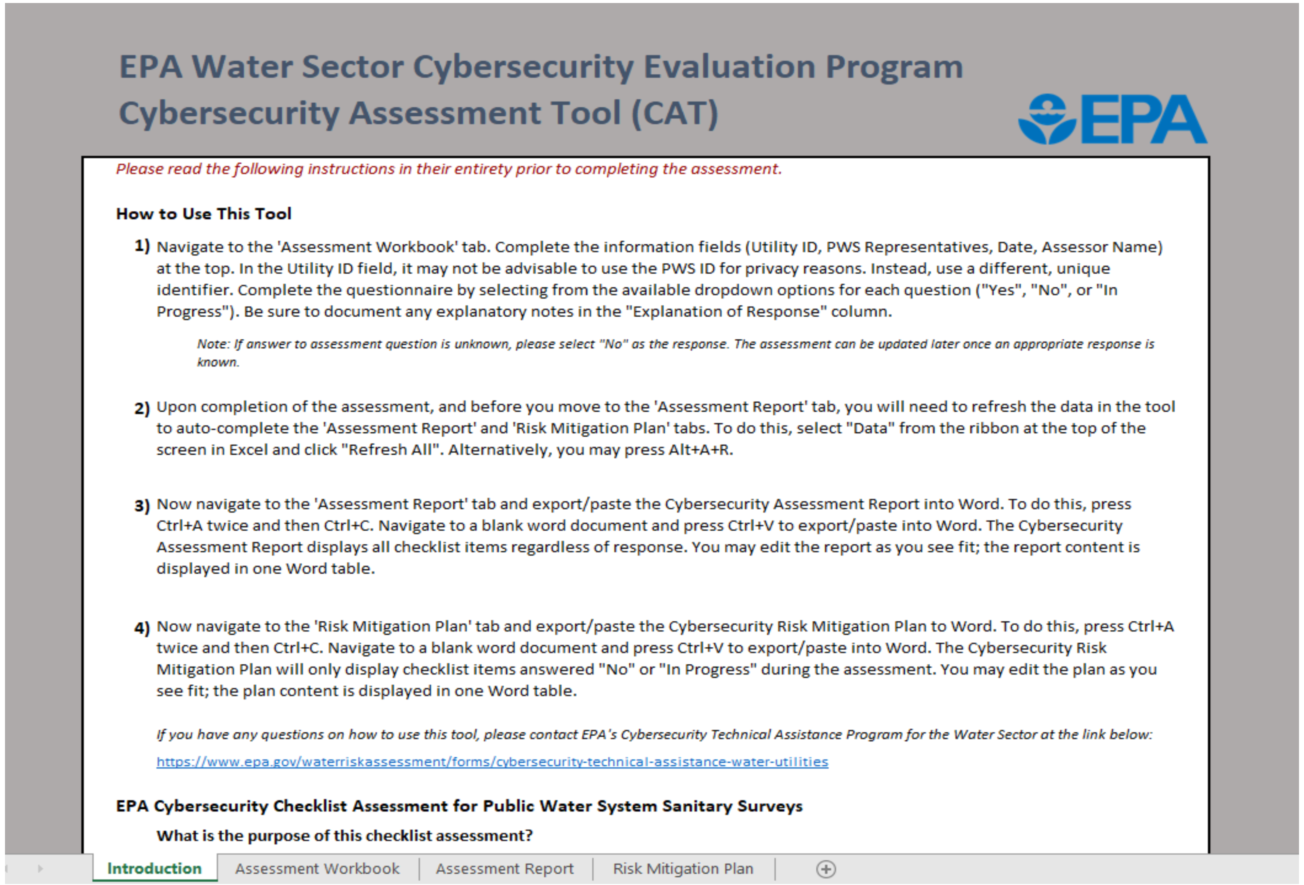
Important Note: States retain their existing authority and discretion to determine when a cybersecurity gap identified during a sanitary survey should be designated as a significant deficiency

EPA Water Cybersecurity Assessment Tool (WCAT)

Provides a method to evaluate cybersecurity at a PWS during a sanitary survey

Includes tabs for:

1. Assessment Workbook
2. Assessment Report
3. Risk Mitigation Plan



EPA Water Sector Cybersecurity Evaluation Program
Cybersecurity Assessment Tool (CAT)

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

How to Use This Tool

1) Navigate to the 'Assessment Workbook' tab. Complete the information fields (Utility ID, PWS Representatives, Date, Assessor Name) at the top. In the Utility ID field, it may not be advisable to use the PWS ID for privacy reasons. Instead, use a different, unique identifier. Complete the questionnaire by selecting from the available dropdown options for each question ("Yes", "No", or "In Progress"). Be sure to document any explanatory notes in the "Explanation of Response" column.

Note: If answer to 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 will need to 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 navigate to the 'Assessment Report' tab and export/paste the Cybersecurity Assessment Report into Word. To do this, press Ctrl+A twice and then Ctrl+C. Navigate to a blank word document and press Ctrl+V to export/paste into Word. The Cybersecurity Assessment Report displays all checklist items regardless of response. You may edit the report as you see fit; the report content is displayed in one Word table.

4) Now navigate to 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. Navigate to a blank word document and press Ctrl+V to export/paste into Word. The Cybersecurity Risk Mitigation Plan will only display checklist items answered "No" or "In Progress" during the assessment. You may edit the plan as you see fit; the plan content is displayed in one Word table.

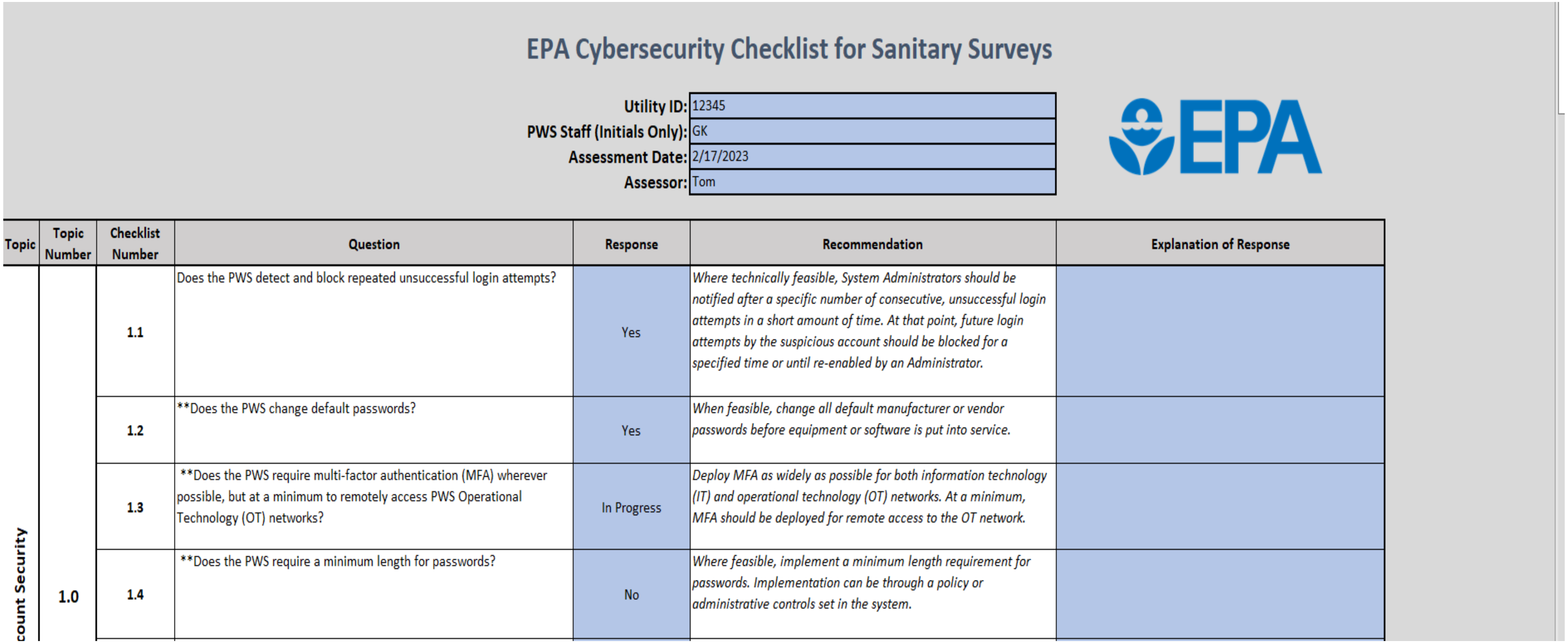
If you have any questions on how to use this tool, please contact EPA's Cybersecurity Technical Assistance Program for the Water Sector at the link below:

https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities

EPA Cybersecurity Checklist Assessment for Public Water System Sanitary Surveys

What is the purpose of this checklist assessment?

Assessment Workbook



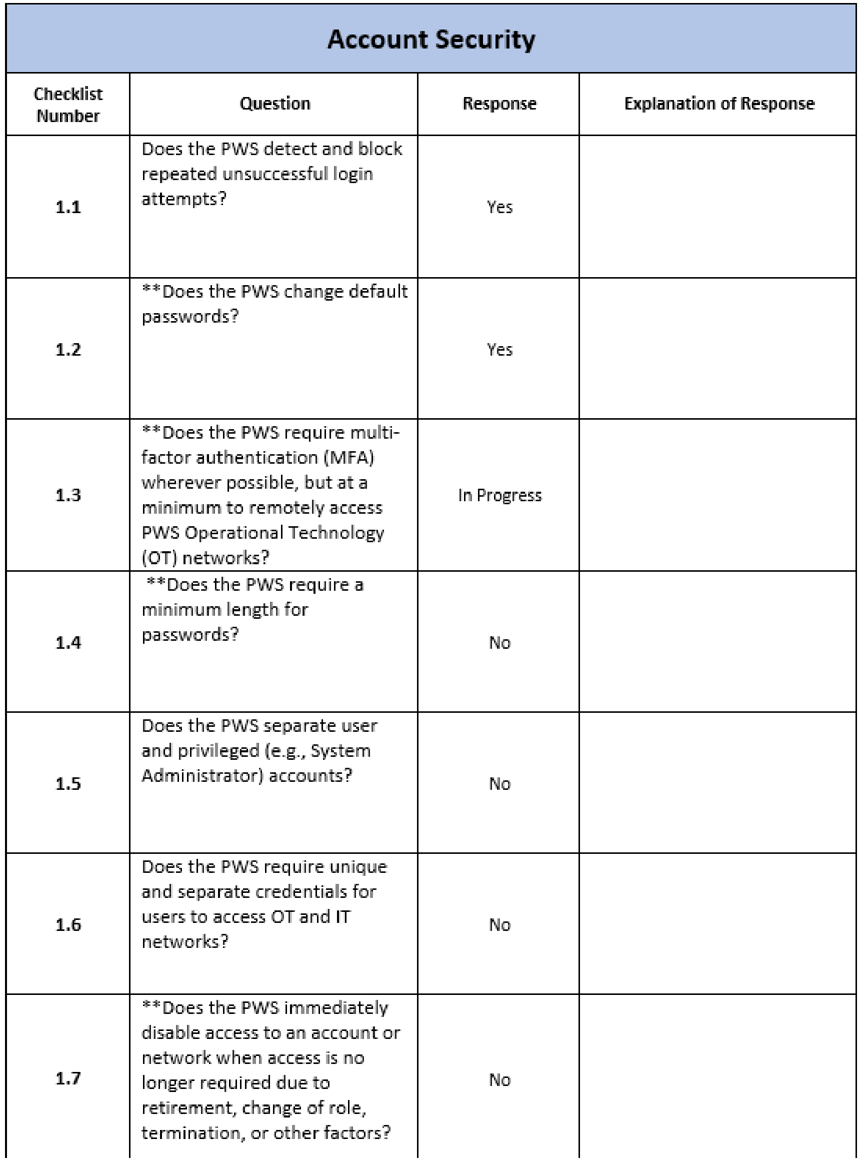
EPA Cybersecurity Checklist for Sanitary Surveys

Utility ID:	12345
PWS Staff (Initials Only):	GK
Assessment Date:	2/17/2023
Assessor:	Tom

Topic	Topic Number	Checklist Number	Question	Response	Recommendation	Explanation of Response
count Security	1.0	1.1	Does the PWS detect and block repeated unsuccessful login attempts?	Yes	*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?	Yes	*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?	In Progress	*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?	No	*Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.*	

Assessment Report Tab

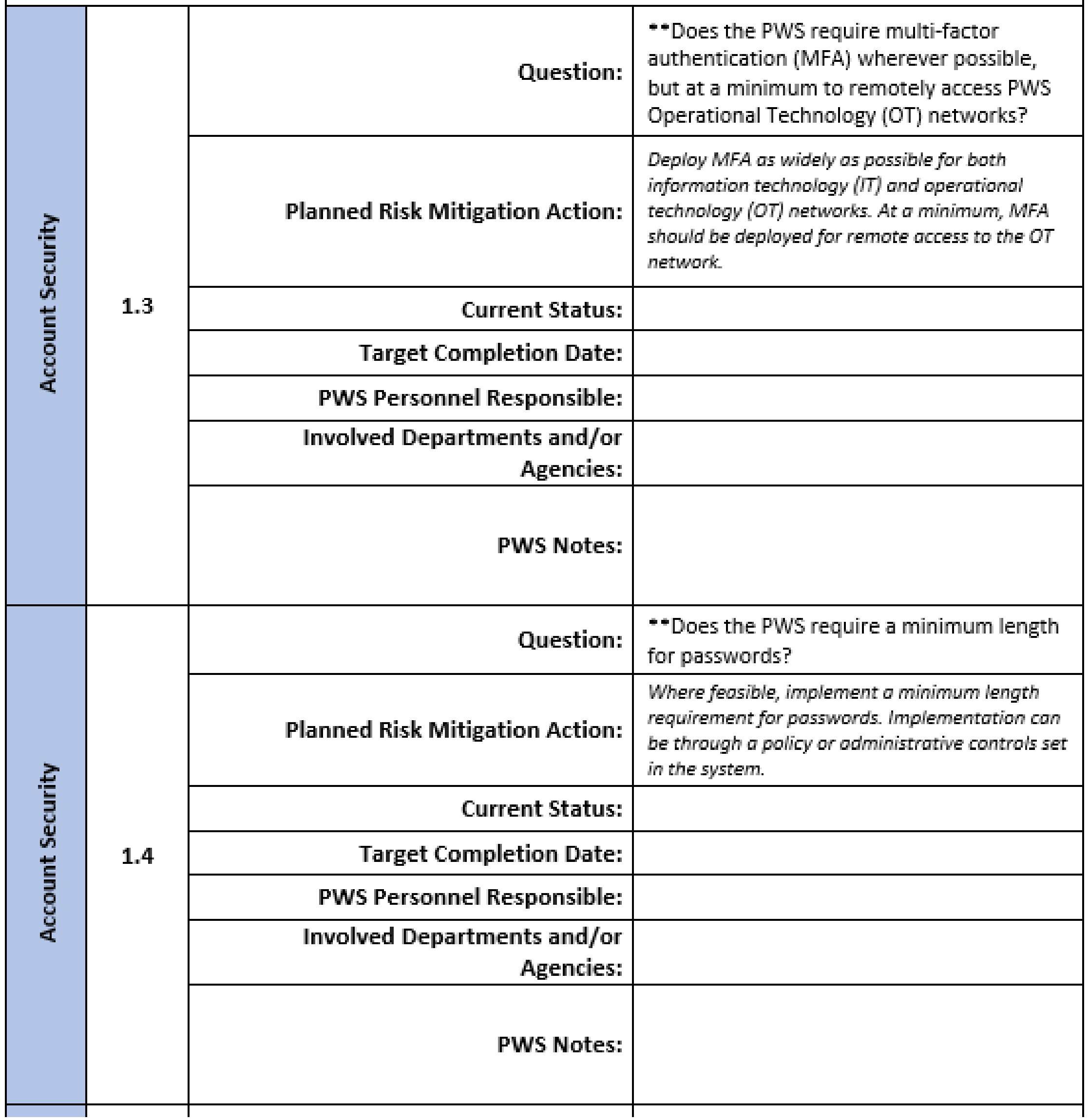
- Provides a summary of results from the completed Cybersecurity Assessment
- Report can be shared with State Surveyor during Sanitary Survey
- Questions indicated with double asterisks (**) represent EPA suggested potential significant deficiencies



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 risk 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:	

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

EPA Water Sector Cybersecurity Evaluation Program

- This program will conduct cybersecurity assessments for PWSs
- Uses the EPA Checklist

- PWSs will receive a report with response to the checklist questions that shows cybersecurity gaps

- The PWS will provide the assessment report to the state to review during the sanitary survey

https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program

Non-EPA Resources Available

- The cybersecurity evaluation during a PWS sanitary survey may be conducted with other government or private-sector assessment methods approved by the state

- Possible alternatives to the EPA Checklist are included in the memo

Possible Government and Private Sector Assessment Methods

- **CISA**
- **NIST**
- **AWWA**
- **ISO**
- **ISA/IEC**

EPA Training

EPA United States Environmental Protection Agency

Office of Water

Future Training Dates

- May 24, 2023 - Webinar
  - Overview of memo and funding options
  - Target audience: Public Water Systems, State Primacy Agencies, other Water Sector partners

Future Training Dates

- APR-SEP In-person/Virtual EPA Regional Workshops
  - Target Audience: State primacy agencies program managers, Direct Implementation Programs managers
  - R1: TBP
  - R2: 6/8/23
  - R3: 4/27/23
  - R4: TBP
  - R5: 6/22/23
  - R6: TBP
  - R7: 8/8/23
  - R8: 10/2/23
  - R9: 5/10 & 5/11/23
  - R10: 8/9/23

Link to our Website and Training

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

EPA United States Environmental Protection Agency

Office of Water