EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems

EPA Office of Water (4608T)
EPA 817-B-23-001
March 2023, Revised August 2024

Disclaimer

The Water Infrastructure and Cyber Resilience Division of the Office of Ground Water and Drinking Water reviewed and approved this document for publication. This document does not impose legally binding requirements on any party. Neither the United States Government nor any of its employees, contractors, or their employees make any warranty, expressed or implied, or assume any legal liability or responsibility for any third party's use of any information, product, or process discussed in this document, or represent that its use by such party would not infringe on privately owned rights. Mention of trade names or commercial products does not constitute endorsement or recommendation for use. Additionally, the guidance provided in this document serves as a voluntary guide to assist water and wastewater entities in assessing, understanding, and combatting cyber risks to their operations, organizational assets, and individuals.

Table of Contents

1.0 Background

1.1. What is the purpose of this publication?

The U.S. Environmental Protection Agency (EPA) developed this publication to assist owners and operators of drinking water and wastewater systems (WWSs) with assessing gaps in their current cybersecurity practices and controls and identifying actions that may reduce their risk from cyberattacks. Further, as described in Section 1.2, community water system (CWS) owners and operators subject to the requirements of the Safe Drinking Water Act (SDWA) section 1433 (as amended by *America's Water Infrastructure Act*) may use this guidance as one option to address cybersecurity in risk and resilience assessments and emergency response plans.

WWSs are frequent targets of malicious cyber activity, which has the potential to interfere with operations and may result in significant response and recovery costs. Of particular concern, a cyberattack on a vulnerable WWS may allow an adversary to manipulate operational technology (OT), which could disrupt the production of clean and safe water. Accordingly, WWS owners and operators should evaluate their cybersecurity practices and controls on a recurring basis and consider steps that may reduce their risk. This will help WWWs from being victimized by a cyberattack and assist with responding if an attack does occur.

Specifically, WWS owners and operators should assess how the use of information technology (IT) and OT in their operations, equipment, and networks, along with the evolution of cybersecurity standards and recommendations, new information about cyber threats, and other considerations, may warrant a reevaluation of their cybersecurity practices and controls. This guidance and the additional technical resources listed in Section 2 can assist WWS owners and operators with this assessment.

1.2. Optional uses of the guidance provided in this publication

EPA recommends that all WWS owners and operators, regardless of system type and population served, evaluate the risks to and resilience of their IT and OT systems to cyber threats and develop risk mitigation plans to address cyber vulnerabilities in critical operations. The guidance in this publication is one method to assist WWS owners and operators with these essential steps:

- Assess current WWS cybersecurity practices and controls to identify significant potential vulnerabilities to cyber threats,
- Develop a plan with specific actions, resources, schedules, and responsibilities to reduce risk from and enhance resilience to cyberattacks, and
- Identify additional resources to assist with improving cybersecurity.

Further, owners and operators of CWSs serving more than 3,300 people are required under SDWA section 1433 to consider cybersecurity when developing or updating *risk and resilience assessments and emergency response plans*. Compliance with SDWA section 1433 requires:

- Assessing the risks to and resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage, and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system; the monitoring practices of the system; the financial infrastructure of the system; the use, storage, or handling of various chemicals by the system; and the operation and maintenance of the system; and may include an evaluation of capital and operational needs for risk and resilience management for the system.
- Preparing or revising, where necessary, an emergency response plan that incorporates the assessment's findings, which shall include strategies and resources to improve the system's resilience, including the system's physical security and cybersecurity.

The guidance in this publication provides one approach that owners and operators of CWSs subject to SDWA section 1433 may follow to meet these requirements. Alternatively, several of the tools and resources from other government and private sector organizations listed in Section 2 of this publication are also effective methods to address cybersecurity under SDWA section 1433.

2.0 Technical Support for Improving Cybersecurity at Water and Wastewater Systems

Technical assistance, guidance, tools, training, and funding that can aid WWS owners and operators with improving cybersecurity are available from EPA and other government and private sector organizations. This section summarizes key programs and resources. Information on additional cybersecurity assistance for WWSs is available on the *EPA Cybersecurity for the Water Sector* website.

This support from both EPA and other government and private sector organizations can assist WWS owners and operators with both identifying gaps in their existing cybersecurity practices and adopting new measures to lower risk and build resilience. Further, it may facilitate addressing cybersecurity in risk and resilience assessments and emergency response plans for CWSs that must comply with SDWA section 1433.

2.1. Cybersecurity Technical Assistance

- EPA's *Cybersecurity Technical Assistance Program for the Water Sector* supports the submission of questions or requests to consult with a subject matter expert on WWS cybersecurity. The planned response time is two business days via email or phone. All assistance is remote.
    - Note: This program does not support cyber incident response or recovery. Reports of cyber incidents will be redirected to the Federal Bureau of Investigation (FBI) or the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA). Other questions outside the scope of this program will be directed to alternate resources.
- EPA's *Water Sector Cybersecurity Evaluation Program* conducts cybersecurity assessments of WWSs. The assessments follow the EPA Cybersecurity Checklist discussed in Section 3. Assessment results are used to develop a cybersecurity risk mitigation plan with prioritized actions.
- *CISA Cybersecurity Advisors (CSAs)* offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal, and territorial governments. CSAs can provide information on CISA cybersecurity products and services and act as liaisons to CISA cyber programs. CSAs also support cyber incident response.
- CISA's *Free Cyber Vulnerability Scanning for Water Utilities* program uses automated tools to conduct vulnerability scanning on external networks. These tools look for vulnerabilities and weak configurations that adversaries could exploit to conduct a cyberattack. EPA recommends that WWSs enroll in this program.
- The U.S. Department of Agriculture Rural Development *Circuit Rider Program* provides technical assistance to rural water systems that are experiencing day-to-day operational, financial or managerial issues. This service is available in each state and territory.

2.2. Cybersecurity Tools and Guidance

- EPA's *Water Cybersecurity Assessment Tool* supports a self-assessment of a WWS for identifying cybersecurity gaps and developing a cybersecurity risk mitigation plan. This program is based on the EPA Cybersecurity Checklist (see Section 3). EPA's *Cybersecurity Technical Assistance Program for the Water Sector* assists a WWS with a third-party cybersecurity assessment and risk mitigation plan development.

- CISA offers several guidance products and tools to strengthen the security and resilience of critical infrastructure facilities, including WWSs, against cyberattacks.
  - CISA's *Water and Wastewater Cybersecurity Toolkit* highlights CISA resources to protect against, and reduce impacts from, cyberattacks.
  - CISA's *Cybersecurity Best Practices* website has information on multiple practice areas and programs for both organizational and personal cybersecurity.
  - CISA's *Cyber Threats and Advisories* website offers current information on cybersecurity threats, threat actors, incident detection and response, and access to *Cybersecurity Alerts and Advisories*, which are updated frequently as new information on cyber threats and vulnerabilities becomes available.
  - The *Cyber Security Evaluation Tool (CSET)* is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and IT network security practices.
  - Similarly, the *Cyber Resilience Review* is an interview-based assessment of an organization's ability to manage cyber risk during normal operations and times of crisis.
- The U.S. Department of Commerce *National Institute of Standards and Technology* (NIST) develops cybersecurity standards and guidelines for critical infrastructure, federal agencies, and the public. The NIST *Cybersecurity Framework* is a voluntary, structured list of cybersecurity outcomes that organizations in all critical infrastructure sectors can use to assess, prioritize, and communicate their cybersecurity efforts.
- The Water Information Sharing and Analysis Center (*WaterISAC*) is a subscription-based service that offers data, case studies, and analysis related to water security threats, including cyber-crime, and provides resources to support response, mitigation, and resilience initiatives.
- The American Water Works Association (*AWWA*) provides many resources to assess cyber risk exposure, establish priorities, and execute a proactive cybersecurity strategy at WWSs.
  - The *Water Sector Cybersecurity Risk Management Guidance* addresses the protection of ICSs at WWSs from cyberattacks.
  - The *Water Sector Cybersecurity Risk Management Tool* uses responses to questions about technology applications at a WWS to generate a prioritized list of controls, which can support identifying and mitigating cybersecurity vulnerabilities.

- The *Water Sector Cybersecurity Risk Management Guidance for Small Systems* is designed to help WWSs serving fewer than 10,000 people, and especially those serving fewer than 3,300 people, improve their cybersecurity practices.

2.3. Cybersecurity Training

- EPA's *Cybersecurity Training* offers both in-person and virtual training on WWS cybersecurity best practices, vulnerability assessments, and risk mitigation plan development.
- The National Rural Water Association (NRWA) offers cybersecurity training and support to help small and rural WWSs serving fewer than 10,000 people.
  - The NRWA *cyber education program* will help small WWSs manage their cybersecurity risk by (1) creating a training program targeted to small systems, (2) training Circuit Riders to help small systems to manage cybersecurity risk, and (3) integrating with other WWS cybersecurity initiatives.
  - NRWA has established a *partnership with WaterISAC* for NRWA members who serve populations of 3,300 or fewer. Eligible members will receive WaterISAC's Security Resilience Update and have access to Water ISAC's monthly Threat Briefing webinars and its Resource Center.

2.4. Cybersecurity Financial Resources

- EPA's *Cybersecurity Funding* webpage provides information on federal programs that provide funding to support cyber resilience at WWSs. Current programs include the *Drinking Water State Revolving Fund*, the *Clean Water State Revolving Fund*, and the *CISA State and Local Cybersecurity Grant Program*.

3.0 EPA Cybersecurity Checklist for Drinking Water and Wastewater Systems

3.1. What is the EPA Cybersecurity Checklist?

The EPA Cybersecurity Checklist (Appendix A) is a series of questions designed to assess the cybersecurity practices and controls at a WWS. The questions are paired with recommended actions to fully implement the practice or control. Certain practices and controls are designated as high priority as discussed in Section 4 below.

The EPA Cybersecurity Checklist was derived from the CISA *Cross-Sector Cybersecurity Performance Goals* (CPGs), which are baseline cybersecurity practices applicable across critical infrastructure sectors and with known risk-reduction value. CISA developed the CPGs in collaboration with each of the 16 critical infrastructure sectors, and they align with the NIST *Cybersecurity Framework*. EPA adapted the CPGs into a simplified question format for use during a WWS cybersecurity assessment.

3.2. How should WWSs use the EPA Cybersecurity Checklist?

The EPA Cybersecurity Checklist questions are intended to identify gaps in baseline cybersecurity at a WWS, which could leave the WWS more vulnerable to an attack. After completing the EPA Cybersecurity Checklist, WWS owners and operators are encouraged to develop a risk mitigation plan to address gaps in cybersecurity practices and controls.

The *Factsheets* in Appendix B have information on implementing the practice or control in each EPA Cybersecurity Checklist question. Additional technical support on adopting practices and controls in EPA's Cybersecurity Checklist is available from EPA's *Cybersecurity Technical Assistance Program for the Water Sector* (described in Section 2).

3.3. What are alternatives to the EPA Cybersecurity Checklist?

Use of the EPA Cybersecurity Checklist is voluntary. As discussed in Section 2, many other government and private sector organizations offer valuable methods and guidance for assessing cybersecurity at a WWS and adopting cybersecurity practices and controls to reduce risk and increase resilience. For WWSs, EPA recommends cybersecurity assessment methods from *CISA*, *NIST*, and *AWWA* (see Section 2 for descriptions), or the adoption of standards from the *International Organization for Standardization* and the *International Society of Automation/International Electrotechnical Commission*.

4.0 Priority Cybersecurity Practices for Water and Wastewater Systems

WWSs have limited cybersecurity resources and may need to prioritize the adoption of risk mitigation actions following an assessment for cybersecurity gaps. EPA, CISA, and the FBI have published the *Top Cyber Actions for Securing Water Systems* (Top Cyber Actions). This factsheet lists eight priority steps that WWS owners and operators should take to reduce cyber risks and improve resilience to cyberattacks.

To support adoption of the Top Cyber Actions, EPA identified the cybersecurity practices and controls from the EPA Cybersecurity Checklist in Appendix A that align with each action. Table 1 shows these practices and controls and associated recommendations from the EPA Cybersecurity Checklist, which are grouped by the corresponding Top Cyber Action.

WWSs are encouraged to adopt the cybersecurity practices and controls in Table 1. Where a WWS is unable to adopt a particular cybersecurity practice or control due to logistical, infrastructure, or other constraints, WWSs should seek alternative or compensating cybersecurity steps to mitigate the vulnerability.

In the EPA Cybersecurity Checklist in Appendix A, as well as in the *Water Cybersecurity Assessment Tool*, the questions and recommendations in Table 1 are designated as priority cybersecurity practices. This designation is also applied in the risk mitigation plan template and

should be considered by WWS owners and operators in the implementation of risk mitigation plans.

Table 1: *Priority Cybersecurity Practices for Water and Wastewater Systems*

Question (Does the WWS…)	Recommendation
1. Reduce Exposure to Public-Facing Internet	
Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminate connections between OT assets and the Internet? **(2.W, 2.X)**	*Recommendation: Eliminate unnecessary exposed ports and services on public-facing assets with regular review and eliminate OT asset connections to the public Internet unless explicitly required for operations.*
2. Conduct Regular Cybersecurity Assessments	
Conduct regular cybersecurity assessments?	*Recommendation: Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.*
Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the WWS? **(1.B)**	*Recommendation: Identify one role/position/title responsible for cybersecurity within the WWS. Whoever fills this role/position/title is then in charge of all WWS cybersecurity activities.*
3. Change Default Passwords Immediately	
Change default passwords and require a minimum length for passwords? **(2.A, 2.B)**	*Recommendation: Change all default manufacturer or vendor passwords before equipment or software is put into service and implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.*
Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access WWS OT and IT networks? **(2.H)**	*Recommendation: Deploy MFA as widely as possible for both OT and IT networks. At a minimum, MFA should be used for remote access to the OT network.*

Question (Does the WWS…)	Recommendation
4. Conduct Inventory of OT/IT Assets	
Maintain an updated inventory of all OT and IT network assets? **(1.A)**	*Recommendation: Regularly review (no less than quarterly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.*
Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets? **(2.O)**	*Recommendation: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version*
5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans	
Have a written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly practiced and updated? **(2.S)**	*Recommendation: Develop, practice, and update an IR plan for cybersecurity incidents that could impact WWS operations. Participate in discussion-based (e.g., TTX) and operations-based (e.g., Drill) exercises to improve responses to potential cyber incidents.*
Have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, Internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterISAC, cyber insurance provider)? **(4.A)**	*Recommendation: Document the procedure for reporting cybersecurity incidents to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats.*
6. Backup OT/IT Systems	
Backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis? **(2.R)**	*Recommendation: Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule:* *3) Keep three copies: one primary and two backups.* *2) Keep the backups on two different media types.* *1) Store one copy offsite.*

Question (Does the WWS…)	Recommendation
7. Reduce Exposure to Vulnerabilities	
Patch or otherwise mitigate known vulnerabilities within the recommended timeframe? **(1.E)**	*Recommendation: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.*
Require unique and separate credentials for users to access OT and IT networks and separate user and privileged (e.g., System Administrator) accounts? **(2.C, 2.E)**	*Recommendation: Require a single user to have two different usernames and passwords; one account to access the IT network, and the other account to access the OT network to reduce the risk of an attacker being able to move between both networks using a single login. Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to ensure accurate information for the individuals who have these privileges.*
Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets? **(2.V)**	*Recommendation: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.*
Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors? **(2.D)**	*Recommendation: Terminate access immediately to accounts or networks upon a change in an individual's status making access unnecessary (e.g., retirement, change in position).*
8. Conduct Cybersecurity Awareness Training	
Provide/conduct annual cybersecurity awareness training for all WWS personnel that covers basic cybersecurity concepts? **(2.I)**	*Recommendation: Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.*

5.0 Artificial Intelligence Risks for Water and Wastewater Systems

The current use of artificial intelligence (AI) by WWSs is limited, but potential advantages of AI for WWS operations and management may drive widespread adoption in the future. Consequently, WWS owners and operators should be aware of the potential advantages, risks, and risk management of AI systems.

AI systems analyze large volumes of historic and real-time data to make decisions and predictions. A properly configured AI system could potentially support, automate, or optimize many business and operational processes at WWSs. Examples could include fine-tuning pump controls, planning system growth, responding quickly to emergency situations, communicating with customers, and monitoring water quality. Future research and deployment of AI systems at WWSs is expected to demonstrate additional areas of beneficial AI use.

However, the deployment of AI systems at WWSs also carries the risk of the AI malfunctioning, either due to an inadvertent cause or a malevolent act. Regardless of cause, if an AI system malfunctions at a WWS, it could make incorrect predictions and decisions that might disrupt water and wastewater services and potentially damage infrastructure.

Inadvertent causes of AI malfunction could include incorrectly installing or training the AI, unexpected data inputs to the AI, or insufficiently trained employees or vendors integrating, monitoring, or interfacing with the AI. An adversary could cause the malfunction or failure of AI by taking control of the AI or feeding the AI corrupt data. Access to AI by adversaries could occur through vectors used in conventional cyberattacks (e.g., weak passwords, social engineering).

In consideration of both the promise and risks of AI, the President issued *Executive Order 14110, "Safe, Secure, And Trustworthy Development and Use of Artificial Intelligence (AI)"* on October 23, 2023. This Executive Order addresses managing and securing AI in critical infrastructure, along with other concerns like protecting privacy and civil liberties and promoting innovation. In keeping with this order, federal agencies are issuing guidance on addressing and managing AI risks to critical infrastructure, including WWSs.

The NIST *Trustworthy & Responsible Artificial Intelligence Resource Center* is an online repository of guidance and training that supports the development and deployment of AI technologies. It includes the NIST *AI Risk Management Framework*, which is intended to increase the trustworthiness of AI systems and foster the responsible development, deployment, and use of AI systems.

This Framework is divided into two parts. Part 1 addresses AI risks and the characteristics of trustworthy systems, which are defined as valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy enhanced, and fair - with their harmful biases managed. Part 2 comprises the "Core" of the Framework. It describes four specific functions to help organizations address the risks of AI systems:

(1) Govern – establish an organizational culture of AI risk management,
(2) Map – understand your individual AI use context and risk profile,
(3) Measure – develop systems to assess, analyze, and manage AI risks, and
(4) Manage – prioritize and act upon AI risks to safety and security.

Each of these functions is broken down into categories and subcategories with specific actions and outcomes.

CISA has published *Mitigating Artificial Intelligence Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators*. The guidelines list ten AI use categories in critical infrastructure, such as automation of operations, performance optimization, event detection, and forecasting. In addition, three categories of system-level AI risk are defined: attacks using AI, attacks targeting AI systems, and failures in AI design and implementation. Risk subcategories and associated mitigation strategies are provided for each risk category. Further, these guidelines are aligned with the NIST AI Risk Management Framework and include recommended actions that critical infrastructure facilities should take in each of the four NIST Framework core functions (listed above).

The factsheet *Deploying AI Systems Securely* was published jointly by the U.S. National Security Agency, CISA, the FBI, the Australian Signals Directorate, the Canadian Centre for Cyber Security, the New Zealand National Cyber Security Centre, and the United Kingdom's National Cyber Security Centre. It was developed to meet three goals: (1) improve the confidentiality, integrity, and availability of AI systems, (2) assure that known cybersecurity vulnerabilities in AI systems are appropriately mitigated, and (3) provide methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

In addition to these currently available guidance materials from the federal government, many private sector organizations offer information on the safe and effective deployment of AI systems in critical infrastructure. WWS owners and operators should be aware of this rapidly advancing technology and consider where deployment of AI systems at their facilities could prove beneficial. Further, they should stay updated on current threats using AI to facilitate cyberattacks on critical infrastructure facilities and incorporate recommended mitigation strategies in their cybersecurity programs.

APPENDIX A: EPA Cybersecurity Checklist for Drinking Water and Wastewater Systems

EPA Cybersecurity Checklist for Drinking Water and Wastewater Systems

Priority cybersecurity practices for Water and Wastewater Systems (WWSs) are denoted with a * after the question.

1. **IDENTIFY.** *Does the WWS…*

1.A. Maintain an updated inventory of all OT and IT network assets?*

Recommendation: Regularly review (no less than quarterly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.

1.B. Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the WWS?*

Recommendation: Identify one role/position/title responsible for cybersecurity within the WWS. Whoever fills this role/position/title is then in charge of all WWS cybersecurity activities.

1.C. Have a named role/position/title that is responsible for planning, resourcing, and executing OT-specific cybersecurity activities?

Recommendation: Identify one role/position/title responsible for ensuring planning, resourcing, and execution of OT-specific cybersecurity activities.

1.D. Provide regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?

Recommendation: Facilitate meetings between OT and IT personnel to provide opportunities for all parties to better understand organizational security needs and to strengthen working relationships.

1.E. Patch or otherwise mitigate known vulnerabilities within the recommended timeframe?*

Recommendation: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.

1.F. This control number is included here to be consistent with the CISA CPG but is not applicable to most WWSs.

1.G/H. Require that all OT vendors and service providers notify the WWS of any security incidents or vulnerabilities in a risk-informed timeframe?

Recommendation: Require vendors and service providers to notify the WWS of potential security incidents and vulnerabilities within a stipulated timeframe described in procurement documents and contracts.

1.I. Include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services?

Recommendation: Include cybersecurity as an evaluation criterion when procuring assets and services. Where feasible, seek out systems that are secure by design and secure by default.

2. **PROTECT.** *Does the WWS…*

2.A. Change default passwords?*

Recommendation: Change all default manufacturer or vendor passwords before equipment or software is put into service.

2.B. Require a minimum length for passwords?*

Recommendation: Implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.

2.C. Require unique and separate credentials for users to access OT and IT networks?*

Recommendation: Require a single user to have two different usernames and passwords; one account to access the IT network, and the other account to access the OT network to reduce the risk of an attacker being able to move between both networks using a single login.

2.D. Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?*

Recommendation: Terminate access immediately to accounts or networks upon a change in an individual's status making access unnecessary (e.g., retirement, change in position).

2.E. 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 ensure accurate information for the individuals who have these privileges.

2.F. Segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g., by IP address and port)?

Recommendation: Require connections between the OT and IT networks to pass through an intermediary, such as a firewall, bastion host, jump box, or demilitarized zone, which is monitored and logged.

2.G. Detect and block repeated unsuccessful login attempts?

Recommendation: Enable System Administrator notification 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.

2.H. Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access WWS Operational Technology (OT)/Information Technology (IT) networks?*

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

2.I. Provide/conduct annual cybersecurity awareness training for all WWS personnel that covers basic cybersecurity concepts?*

Recommendation: Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.

2.J. Offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties?

Recommendation: Provide specialized OT-focused cybersecurity training to all personnel who use OT assets.

2.K. Use effective encryption to maintain the confidentiality of data in transit?

Recommendation: When sending information and data, use Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption standards.

2.L. Use encryption to maintain the confidentiality of stored sensitive data?

Recommendation: Do not store sensitive data, including credentials (i.e., usernames and passwords) in plain text files.

2.M. Use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?

Recommendation: Ensure that email security controls are enabled on all corporate email infrastructure.

2.N. Disable Microsoft Office macros, or similar embedded code, by default on all assets?

Recommendation: Disable embedded macros and similar executable code by default on all assets.

2.O. Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?*

Recommendation: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version.

2.P. Maintain updated documentation describing network topology (i.e., connections between all network components) across WWS OT and IT networks?

Recommendation: Maintain complete and accurate documentation of all WWS OT and IT network topologies to facilitate incident response and recovery.

2.Q. Require approval before new software is installed or deployed?

Recommendation: Only allow Administrators to install new software on a WWS-issued asset.

2.R. Backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?*

Recommendation: Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule:

3) Keep three copies: one primary and two backups;
2) Keep the backups on two different media types;
1) Store one copy offsite.

2.S. Have a written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly practiced and updated?*

Recommendation: Develop, practice, and update an IR plan for cybersecurity incidents that could impact WWS operations. Participate in discussion-based (e.g., TTX) and operations-based exercises (e.g., Drill) to improve responses to potential cyber incidents.

2.T. Collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?

Recommendation: Collect and store logs and/or network traffic data to aid in detecting cyberattacks and investigating suspicious activity.

2.U. Protect security logs from unauthorized access and tampering?

Recommendation: Store security logs in a central system or database that can only be accessed by authorized and authenticated users.

2.V. Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?*

Recommendation: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.

2.W. Ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol)?*

Recommendation: Eliminate unnecessary exposed ports and services on public-facing assets and regularly review.

2.X. Eliminate connections between OT assets and the Internet?*

Recommendation: Eliminate OT asset connections to the public Internet unless explicitly required for operations.

3. **DETECT.** *Does the WWS…*

3.A. Keep a list of threats and adversary tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the WWS?

Recommendation: Receive CISA alerts, prioritize the Known Exploited Vulnerabilities (KEV) list, and maintain documentation of TTPs relevant to the WWS.

4. **RESPOND.** *Does the WWS…*

4.A. Have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, Internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterISAC, cyber insurance provider)?[1]*

Recommendation: Document the procedure for reporting cybersecurity incidents to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats.

4.B. This control number is included here to be consistent with the CISA CPGs but is not applicable to most WWSs.

4.C. This control number is included here to be consistent with the CISA CPGs but is not applicable to most WWSs.

[1]Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA is required to issue regulations, through notice-and-comment rulemaking, requiring covered entities to report covered cyber incidents and ransom payments made as a result of a ransomware attack to CISA. CISA's Notice of Proposed Rulemaking proposes applying these requirements to at least some entities in the Water and Wastewater Sector. This recommendation will be revised as necessary when the CIRCIA Final Rule is issued.

5. **RECOVER.** *Does the WWS…*

5.A Have the ability to safely and effectively recover from a cybersecurity incident?

Recommendation: Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.

APPENDIX B: EPA Checklist Factsheets

The EPA Checklist Factsheets can be found on EPA's *Factsheets* webpage.

APPENDIX C: Glossary of Terms

Term	Definition
Access Control Lists	Lists that identify individuals who can access an Operational Technology (OT) and/or Information Technology (IT) system.
Active Services	Programs running in the background.
Artificial Intelligence	The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.
The Artificial Intelligence Risk Management Framework (AI RMF)	A framework developed by the National Institute of Science and Technology (NIST) that is intended to help developers, users and evaluators of AI systems better manage AI risks which could affect individuals, organizations, society, or the environment.
Asset	A cyber facility, device, information, or process that has value.
Automatic Account Lockout or Account Lockout Threshold	Policy that determines how many times a person can attempt to log in with incorrect credentials before the system locks them out.
Bastion Host	A special-purpose computer on an OT or IT network that a WWS specifically designs and configures to withstand cyberattacks.
Backup	The process of creating a copy of critical WWS data that can be used for recovery in case the original data is lost or corrupted.
Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisors (CSAs)	Professionals that provide cybersecurity assistance to critical infrastructure owners, including WWSs, such as cyber preparedness, assessments and protective resources, and incident coordination and support.
Community Water System (CWS)	A public water system that supplies water to the same population year-round.

Term	Definition
Compensating Controls	Security and privacy controls that a WWS implements in lieu of the baseline controls. Compensating controls provide equivalent or comparable protection for an OT or IT system.
Configuration	The setup of an OT or IT system or component, including the conditions, parameters, and specifications.
Control	A practice or measure that a WWS uses to prevent, detect, and mitigate cyber threats and attacks. Practices range from physical controls, such as removing USB ports in laptops, to technical controls, such as using firewalls and multi-factor authentication.
Control System	A system that assists in implementing a procedure or process (e.g., water treatment). Control systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Programmable Logic Controllers (PLCs), and other types of industrial control systems.
Credentials	Information that is unique to a specific user and is required to log on to a system or a program. For example, a username and password.
Data Loss Prevention (DLP)	The practice of detecting and preventing data breaches, exfiltration (theft or unauthorized removal or movement of any data from a device), or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and to comply with regulations.
Demilitarized Zone (DMZ)	A perimeter network that acts as a fence and governs the exchange of information between internal and external computer networks. It regulates how information flows from an internal network to an external network and who from the external network can access the internal network. It is often used between the OT and IT networks of a WWS.

Term	Definition
Cybersecurity and Infrastructure Security Agency (CISA)	CISA leads the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure. CISA develops and publishes a variety of information, resources, tools, and training for the water sector and other critical infrastructure sectors.
Devices	Pieces of computer hardware that include desktops, laptops, servers, and tablets.
DomainKeys Identified Mail (DKIM)	Email authentication method to verify the authenticity of emails.
Domain-Based Message Authentication, Reporting, and Conformance (DMARC)	A protocol that uses Sender Policy Framework (SPF) and/or DKIM records to authenticate emails. It allows for the rejection of fraudulent emails.
Embedded Code	Code that a third-party website, such as YouTube or X (formerly known as Twitter), generates that a user can copy and paste into their own webpage. This embedded code will then show the same media, application, or feed on the user's webpage as it does on the original website.
Emergency Response Plan (ERP)	A plan that describes strategies, resources, other plans, and procedures WWSs can use to prepare for and respond to a natural or man-made incident that threatens life, property, or the environment.
Encrypt	Process by which a WWS converts plain text or data into coded or "ciphered" text/data.
Encryption	Any procedure that a WWS uses to convert plain text or data into coded or "ciphered" text/data to prevent anyone but the intended recipient from decoding and reading the text or data.
Executable	A piece of computer code or programming that can perform set tasks according to its encoded instructions. Executable files are used by a computer program or routine.

Term	Definition
Fast Identity Online (FIDO)/Client to Authenticator Protocol (CTAP)	Developed by the FIDO Alliance, the CTAP enables communication without the use of passwords between an external authenticator (e.g., mobile phones, connected devices) and another client (e.g., browser) or platform (e.g., operating system such as Microsoft Windows).
FBI Internet Crime Complaint Center (IC3)	A division of the Federal Bureau of Investigation focused on suspected Internet-facilitated criminal activity.
Firewall	A device that restricts data communication between two connected networks. A firewall may be either an application installed on a general-purpose computer or a separate device that allows or rejects information flow between networks. Typically, a WWS uses firewalls to define zone borders, such as between OT and IT systems at a WWS.
Firmware	Software program or instructions programmed on the flash read-only memory (ROM) of a hardware device. It enables the device to communicate with other computer hardware.
Group Policy Object (GPO)	Allows a System Administrator to dictate how users and computers will interact. Group policies are primarily security tools and a WWS can use them to apply security settings to users and computers, such as requiring a minimum password length.
Human-Machine Interface (HMI)	User interface or dashboard that connects a user to a machine, system, or device. The term “HMI” is commonly used in the context of an industrial process, such as interacting with a SCADA system. For example, a WWS operator might use an HMI to check if a certain pump is operating.
Internet Protocol (IP) Address	A numerical address that identifies a device on the Internet or local network.

Term	Definition
Incident Response (IR) Plan	A set of predetermined and documented procedures to detect and respond to a cyber incident. Some WWSs may include their cybersecurity IR plan as part of their WWS Emergency Response Plan.
Information Sharing and Analysis Centers (ISACs)	An organization that collects, analyzes, and disseminates actionable threat information to its members and provides them with tools to mitigate risks and improve resiliency. For example, WaterISAC provides these services to WWSs.
Information System	Interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
Information Technology (IT)	A set of resources that an organization uses for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Industrial Control System (ICS)	A system used to control industrial processes such as water treatment and distribution. ICSs include SCADA systems (frequently used at WWSs to control geographically dispersed assets), DCSs, and smaller control systems using PLCs to control localized processes.
Interception	Interception allows attackers to access data, applications, or systems, and are primarily attacks against confidentiality. This could be unauthorized file viewing or copying, eavesdropping on phone conversations, or reading another person's email. These attacks can be conducted against data at rest (e.g., stored on a server) or in motion (e.g., an email in transit from sender to receiver).
International Electrotechnical Commission (IEC)	A global, not-for-profit membership organization that brings together 173 countries and coordinates the work of 20,000 experts globally. It facilitates electricity access,

Term	Definition
	and verifies the safety, performance and interoperability of electric and electronic devices and systems, including consumer devices such as mobile phones, refrigerators, office and medical equipment, IT, electricity generation, and more.
International Society of Automation (ISA)	A non-profit professional association founded in 1945 to create a better world through automation. ISA develops widely used global standards, certifies professionals, provides education and training, publishes books and technical articles, hosts conferences and exhibits, and provides networking and career development programs for its members and customers.
International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443	The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the IEC, provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).
Intranet	A local communications network that is often used to improve communication, collaboration, and engagement within an organization. It typically excludes anyone from outside the organization.
Intrusion Detection System/Intrusion Protection System (IDS/IPS)	Both systems are placed within a network to alert when an unwanted intrusion has occurred. An IDS is designed to only provide an alert about a potential incident. An IPS, on the other hand, acts to block the attempted intrusion or otherwise remediate the attack.
Inventory	The formal listing or record of the organizational property at a WWS.
Jump Box	A hardened and monitored device that spans two dissimilar network security zones and provides a controlled means of access between them. It essentially serves as a gated bridge between the zones.

Term	Definition
Known Exploitable Vulnerabilities (KEV) Catalog	A list of vulnerabilities that CISA has identified as being exploited or that threat actors have used to conduct attacks.
Log	A record of the events occurring within a WWS's OT and IT systems and networks.
Media Access Control (MAC) Address	A unique identifier assigned to a network interface controller (NIC) for use as a network address. Device manufacturers typically assign MAC addresses, so devices come with this address already assigned to them, unlike IP addresses. Also referred to as the hardware address or physical address.
Macro	A configured action that allows users to automate tasks and add functionality in files (e.g., a command button and an associated macro on a form). The macro contains the commands that the button will perform each time a user clicks it.
MITRE ATT&CK	A guideline for classifying and describing cyberattacks and intrusions.
Multi-factor Authentication (MFA)	A feature that requires more than one distinct authentication factor, such as a code texted to a cell phone, to activate a device or login into an account.
National Vulnerability Database (NVD)	The NVD was established to provide a U.S. government data repository about software vulnerabilities and configuration settings.
Network Segmentation	Dividing a network into multiple segments or "subnets," each acting as its own small network. This feature allows for control of the information flow between subnets. WWSs can use segmentation to improve monitoring, boost performance, localize technical issues, and enhance cybersecurity.

Term	Definition
National Institute of Standards and Technology (NIST)	An organization that develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public.
NIST Cybersecurity Framework (CSF)	Voluntary guidance, based on existing standards, guidelines, and practices, for organizations such as WWSs to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, NIST designed the CSF to foster risk and cybersecurity management communications between internal and external organizational stakeholders.
Network Switch	A device that connects users, applications, and equipment across a network so that they can communicate with one another and share resources.
Network Traffic	The amount of data that moves across a network during any given time.
Operating System (OS)	Software that serves as an interface between computer hardware and the user. Applications (e.g., Microsoft Office) require an environment to operate and perform tasks in. The OS helps users interact with applications and other hardware and programs. OS also performs tasks such as file, memory, and process management.
Operational Technology (OT)	The hardware, software, and firmware components of a system that a WWS uses to detect or cause changes in physical processes through the direct control and monitoring of physical devices. For many WWSs, this is a SCADA system.
Patches	Software and operating system updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs and provide enhanced security features.

Term	Definition
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred.
Protected Critical Infrastructure Information (PCII) Program	The PCII Program protects information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, or other information from federal, state, and local disclosure laws. This allows partners such as WWSs to securely share their critical infrastructure information with CISA without fear of disclosure.
Phishing	Fraudulent emails, text messages, phone calls or websites that trick people into downloading malware, sharing sensitive information (e.g., Social Security and credit card numbers, bank account numbers, login credentials), or taking other actions that expose themselves or their WWS to cybercrime.
Privileged Account	A user account that has more privileges than ordinary users. Privileged accounts might, for instance, be able to install or remove software, upgrade the operating system, or modify system or application configurations. These accounts might also have access to files that standard users are not able to access. At a WWS, a "System Administrator" would most likely have a privileged account.
Programmable Logic Controller (PLC)	A small industrial computer originally designed to perform the logic functions executed by electrical hardware (e.g., relays, switches, and mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and WWSs frequently use them in SCADA systems.
Purdue Enterprise Reference Architecture (PERA), or Purdue Model	A six-layer model for ICS network segmentation that defines the system components found in each of the layers and the network boundary controls for securing each layer and ultimately the ICS network.

Term	Definition
Remote Desktop Protocol (RDP)	A network communications protocol developed by Microsoft. It enables System Administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers. Support technicians often use RDP to diagnose and repair a user's system remotely.
Risk and Resilience Assessment (RRA)	An assessment of the risks to the WWS, including malevolent acts and natural hazards, and resilience to those risks.
Router	A device that communicates between the Internet and the devices at a WWS that connect to the Internet.
Server	A computer program or device that provides a service (such as sharing data or resources) to another computer program and its user, also known as the client.
Supervisory Control and Data Acquisition (SCADA)	A type of industrial control system. It is a collection of both software and hardware components that allows users to control, monitor, and automate processes. SCADA systems help to gather and analyze real-time data.
Secure Sockets Layer (SSL)	A protocol that a WWS uses for protecting private information during transmission via the Internet.
Sender Policy Framework (SPF)	An email authentication method that helps protect outgoing email from being marked as spam by receiving organizations.
Service Level Agreement (SLA)	A commitment between a service provider (e.g., vendor) and a customer (e.g., WWS). Aspects of the service's quality and availability, as well as the parties' individual responsibilities, are agreed upon in advance.
Spoofing	A type of scam in which an attacker disguises an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source.

Term	Definition
Software	A collection of data, programs, and instructions used to operate computers and execute specific tasks, encompassing everything from operating systems to various applications, essential for performing a wide range of digital functions.
Start Transport Layer Security (STARTTLS)	A protocol used to ensure email is securely transported from one server to another.
Supply Chain Attack	A type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Supply chain attacks are difficult to detect, as they rely on software that has already been trusted and can be widely distributed (e.g., SolarWinds attack).
System Administrator	Person responsible for managing, updating, and operating the computer system(s). This person can be an individual at the WWS or a vendor.
Security Information and Event Management (SIEM)	A tool that collects event log data from a range of sources (e.g., devices, software), identifies activity that deviates from “normal” with real-time analysis, and takes appropriate action. It helps organizations detect, analyze, and respond to security threats before they interrupt operations.
Tabletop Exercise (TTX)	A discussion-based exercise where personnel with roles and responsibilities in a particular IR plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during a cyber emergency and their responses to a particular cyber incident. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
Tactics, Techniques, and Procedures (TTPs)	This is the term used by cybersecurity professionals to describe the behaviors, processes, actions, and strategies used by an attacker to engage in cyberattacks.

Term	Definition
Transparent Data Encryption (TDE)	TDE enables the user to encrypt sensitive data that is stored in databases at the file level. It protects data at "rest", not data in "transit."
Transport Layer Security (TLS)	An authentication and encryption protocol widely implemented in browsers and Web servers. Hyper Text Transfer Protocol (HTTP) traffic (a standard method for communication between clients and Web servers) transmitted using TLS is known as Hyper Text Transfer Protocol Secure (HTTPS).
U.S. Department of Agricultural (USDA) Rural Development (RD) Circuit Rider Program	Circuit Riders provide technical assistance to rural water systems on operational, financial, and/or managerial topics.
Virtual Private Network (VPN)	A service that extends a private network across a public network (e.g., Internet) and provides a secure, encrypted channel between the user's device and the private network. A VPN allows users to conduct work remotely.
Vulnerability	A flaw or weakness in a piece of software or firmware that an attacker can use to modify application code, damage an asset, gain access to a network, or execute other malicious activity.
Wireless Access Point	A device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub and projects a WiFi signal within a designated area.