Guidance on Risk and Resilience Assessments for Small Community Drinking Water Systems

What is the Purpose of this Guidance?

This guidance will help small community water systems (CWSs) serving greater than 3,300 but less than 50,000 people to meet the requirements for risk and resilience assessments (RRAs) under section 1433 of the Safe Drinking Water Act (SDWA), which was amended by America's Water Infrastructure Act (AWIA) section 2013 in 2018.

This guidance does not address emergency response plans (ERPs), which are also required for CWSs that serve over 3,300 under SDWA section 1433. EPA has developed an ERP Template and Instructions for Drinking Water Utilities to help develop ERPs. The results of this RRA should be used to develop your ERP.

Further, this guidance does not cover all aspects of water system security and resilience, such as asset management, climate change, and emergency preparedness and response. Visit EPA's Drinking Water and Wastewater Resilience page to find more information on water system security and resilience. This information includes EPA's Resilient Strategies Guide, which assists drinking water and wastewater utilities with adaption planning for climate change.

Who Should Use this Guidance?

This guidance is intended to help small CWSs serving greater than 3,300 but less than 50,000 people to comply with the requirements for RRAs in SDWA section 1433. For larger CWSs, EPA recommends the Vulnerability Self-Assessment Tool (VSAT) or an alternate risk assessment method. Additional information on water system security and resilience can be found on EPA's Drinking Water and Wastewater Resilience page as well as the Cybersecurity and Infrastructure Security Agency's (CISA's) Water and Wastewater Cybersecurity page.

SDWA section 1433 does not require the use of any standards, methods, or tools for the RRA or ERP. Thus, this guidance is an optional resource that utilities may use to facilitate a sound RRA; it is not required. Each CWS is responsible for ensuring that the RRA and ERP address all the criteria in SDWA section 1433(a) and (b).

CWSs serving 3,300 or fewer people and non-community water systems are not required to conduct RRAs under SDWA. EPA recommends, however, that these water systems use this or other guidance to learn how to conduct RRAs and address threats from malevolent acts and natural hazards that threaten safe drinking water.

What are the RRA Requirements in SDWA Section 1433?

SDWA section 1433 requires CWSs serving more than 3,300 people to assess the risks to and resilience of the system to malevolent acts and natural hazards. The law specifies CWS assets (e.g., infrastructure) that the assessment must address. These assets are listed in Tables 1a – 10b in the *Risk and Resilience Assessment Checklist* (see fillable PDF checklist below beginning on page 1 or fillable Word checklist embedded on page iv).

CWSs must review, revise where applicable, and re-certify their RRA and ERP to EPA every five years from the original deadlines specified in the law. See the table below for the upcoming five-year submission cycle RRA and ERP deadlines.

Population Served	Upcoming RRA Certification Deadline	Upcoming ERP Certification Deadline*
≥100,000	March 31, 2025	September 30, 2025
50,000-99,999	December 31, 2025	June 30, 2026
3,301-49,999	June 30, 2026	December 31, 2026

*ERP certifications are due six months from the date of the RRA certification. The dates shown above are certification dates based on a CWS submitting a RRA on the final due date.

NOTE: CWSs do not submit the actual RRA to EPA. Visit EPA's informational page on How to Certify Your RRA or ERP for instructions on how to certify. Every five years, CWSs must review the RRA, revise it as needed, and provide a new certification to EPA.

What are Risk and Resilience in a CWS?

Risk to critical infrastructure, including CWSs, is a function of **threat likelihood**, **vulnerability**, and **consequence**.

- **Threat** can be a malevolent act, like a cyberattack or process sabotage, or a natural hazard, such as a flood or hurricane.
- **Threat likelihood** is the probability that a malevolent act will be carried out against the water system or that a natural hazard will occur.
- **Vulnerability** is a weakness that can be exploited by an adversary or impacted by a natural hazard. It is the probability that if a malevolent act or a natural hazard occurred, then the water system would suffer significant adverse impacts.
- **Consequences** are the magnitude of loss that would ensue if a threat had an adverse impact against a water system. Consequences may include:
    - Economic loss to the water system from damage to CWS assets
    - Economic loss to the CWS service area from a service disruption, and
    - Severe illness or deaths that could result from water system contamination, a hazardous gas release, or other hazard involving the water system.

Resilience is the capability of a water system to maintain operations or recover when a malevolent act or a natural hazard occurs.

Countermeasures are mitigation steps that a water system implements to reduce risk and increase resilience. They may include plans, equipment, procedures, and other measures.

How Does a CWS Assess Risk and Resilience Under SDWA Section 1433?

Tables 1a – 10b in the *Risk and Resilience Assessment Checklist* (see fillable checklist below beginning on page 5 or fillable Word checklist imbedded on page 4) list the categories of water system assets that you must assess under SDWA section 1433. In all tables (i.e., for all asset categories), do the following:

1. Select the **malevolent acts** from those listed in the table that pose a significant risk to the asset category at the CWS. You may write-in malevolent acts not listed in the table.
    - Focus the selection of malevolent acts on those that are prevalent in the United States (e.g., cyber-attacks), can exploit vulnerabilities at the CWS (e.g., known security gaps), and have the potential for significant economic or public health consequences (e.g., contamination).

NOTE: EPA's Baseline Information on Malevolent Acts Relevant to Community Water Systems assists water systems with estimating the likelihood of these malevolent acts and provides resources for additional information.

2. For each malevolent act that you identify as a significant risk, briefly describe how the malevolent act could impact the asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include major assets that might be damaged or disabled, water service restrictions or loss, and public health impacts as applicable.
3. Select the **natural hazards** from those listed in the table that may pose a significant risk to the asset category at the CWS. You may write-in natural hazards not listed in the table.
    - Focus the selection of natural hazards on those that are prevalent in the area where the water system is located, may affect vulnerable water system infrastructure, and have the potential for significant economic or public health consequences related to the CWS.
4. For each natural hazard that you identify as a significant risk, briefly describe, or provide examples of how the hazard could impact the asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include major assets that might be damaged or disabled, water service restrictions or loss, and public health impacts as applicable.
5. **Table 11: Checklist of Priority Cybersecurity Practices for Water Systems** can be used to evaluate cybersecurity best practices at a CWS. This checklist is extracted directly from a subset of the Cybersecurity and Infrastructure Agency (CISA) Cross-Sector Cybersecurity Performance Goals. In this checklist, a subset of

the Cybersecurity Performance Goals that reflect essential cybersecurity best practices are written in a question format to facilitate evaluating a CWS. Alternatives to this checklist include cybersecurity evaluation methods and standards from CISA[1], NIST[2], AWWA[3], ISO[4], and ISA/IEC[5].

To complete the Cybersecurity Checklist, read each "Does the CWS…" question and mark the appropriate check box ("Yes", "No", "In progress", "Not applicable"). For each question marked with a "No", the table contains a recommended action to address the question.

6. **OPTIONAL Table 12: Countermeasures** provides a table for you to identify countermeasures that the CWS could potentially implement to reduce risk from the malevolent acts and natural hazards based on the information that you entered into tables 1a – 10b of this assessment.
    - For malevolent acts, countermeasures are intended to deter, delay, detect, and respond to an attack.
    - For natural hazards, countermeasures are intended to prepare, respond, and recover from an event.

NOTE: A single countermeasure (e.g., emergency response planning or power resilience) may reduce risk across multiple malevolent acts, natural hazards, and asset categories.

Importance of Addressing Cybersecurity

Thoroughly addressing cybersecurity is essential in your CWS's RRA. In EPA's Baseline Information on Malevolent Acts Relevant to Community Water Systems, cybersecurity has an annual threat likelihood value of 100%, underscoring the prevalence of cyberattacks on CWSs in the United States. Cyberattacks are the highest-risk malevolent act carried out against water systems (and other critical infrastructure).

Cybersecurity is a required element in your RRA according to SDWA section 1433. The risks from and resilience to cyberattacks against the asset categories listed in SDWA 1433(a) must be addressed where applicable (asset categories at CWSs that do not involve electronic monitoring or control may not be at risk from cyberattacks). In addition, CWSs should complete Table 11, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

If a CWS would prefer to have assistance assessing cybersecurity in their RRA, they may participate in EPA's Water Sector Cybersecurity Evaluation Program. EPA will conduct a free cybersecurity assessment using EPA's Cybersecurity Checklist for water and wastewater systems to identify cybersecurity gaps and vulnerabilities. Utilities who participate in the program will receive an Assessment Report and a Risk Mitigation Plan template in a secure file that can be added to their RRA.

For more information and resources related to cybersecurity, please visit EPA Cybersecurity for the Water Sector.

July 2024 Updates

EPA originally published this *Guidance on Risk and Resilience Assessments for Small Community Drinking Water Systems* in May 2020. This document was updated in July 2024 to incorporate updates to version 3.0 of EPA's *Baseline Information on Malevolent Acts Relevant to Community Water Systems* and to assist CWSs with reviewing and, as needed, revising their RRAs in anticipation of the upcoming certification deadlines. Here is a summary of the updates made to the May 2024 version:

- "Cyberattack on Process Control Systems" and "Cyberattack on Business Enterprise Systems", which were presented as separate malevolent acts in the original version, have been combined into a single threat, "Cyberattack".
- "Accidental Contamination" of source and finished water, which were presented as malevolent acts in the original version, have been eliminated (intentional contamination threats were retained).
- The definition of "Electronic, Computer, or Other Automated Systems" has been updated to align with terminology commonly used in the cybersecurity field.
- Added Table 11, "Checklist of Priority Cybersecurity Practices for Water Systems" to provide a method to evaluate cybersecurity at a CWS using CISA's Cross-Sector Cybersecurity Performance Goals.

---

1 CISA Cyber Resilience Review

2 NIST Cybersecurity Framework

3 American Water Works Association (AWWA), Cybersecurity Assessment Tool and Guidance

4 International Organization for Standardization (ISO), 27001 Information Security Management

5 International Society of Automation (ISA)/International Electrotechnical Commission (IEC), 62443 series of standards

Complete the CWS Risk and Resilience Assessment Checklist

EPA offers the CWS *Risk and Resilience Assessment Checklist* in two formats. A fillable PDF format is provided on the pages that follow. This format has fixed fields and may not be changed by the user. Alternatively, a Word version may be accessed by clicking on the icon below. The Word version may be changed by the user. To access the Word version, the PDF file must first be downloaded to your computer and opened in a PDF reader. **The content of the PDF and Word versions is the same.**

CWS Risk and Resilience Assessment Checklist

Community Water System
Risk and Resilience Assessment Checklist

Enter CWS Name Below:

_____

Risk and Resilience Assessment

Please fill in the information below.

Facility Name (if applicable)**:**

PWSID:

Description of System:

Analyst Name(s):

Date of Analysis:

Analysis Notes:

Table 1a: Physical Barriers (Malevolent Acts)[6]

Asset Category: *Physical Barriers* **Examples of Assets in this Category:** Encompasses physical security in place at the CWS. Possible examples include fencing, bollards, and perimeter walls; gates and facility entrances; intrusion detection sensors and alarms; access control systems (e.g., locks, card reader systems); and hardened doors, security grilles, and equipment cages.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Physical Barriers* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[7]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Other(s), enter below:	

[6] In a risk assessment, physical barriers are usually treated as countermeasures, which reduce the risk of a threat to an asset, rather than being treated as assets. However, under AWIA, a CWS must assess the risks to and resilience of physical barriers.

[7] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Table 1b: Physical Barriers (Natural Hazards)[8]

Asset Category: *Physical Barriers* **Examples of Assets in this Category:** Encompasses physical security in place at the CWS. Possible examples include fencing, bollards, and perimeter walls; gates and facility entrances; intrusion detection sensors and alarms; access control systems (e.g., locks, card reader systems); and hardened doors, security grilles, and equipment cages.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Physical Barriers* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

[8] In a risk assessment, physical barriers are usually treated as countermeasures, which reduce the risk of a threat to an asset, rather than analyzed as assets themselves. However, under AWIA, a CWS must assess the risks to and resilience of physical barriers.

Table 2a: Source Water (Malevolent Acts)

Asset Category: *Source Water* **Examples of Assets in this Category:** Encompasses all sources that supply water to a water system. Possible examples include rivers, streams, lakes, source water reservoirs, groundwater, and purchased water.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Source Water* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Theft or Diversion – Physical	
☐ Intentional Contamination of Source Water	
☐ Other(s), enter below:	

Table 2b: Source Water (Natural Hazards)

Asset Category: *Source Water* **Examples of Assets in this Category:** Encompasses all sources that supply water to a water system. Possible examples include rivers, streams, lakes, source water reservoirs, groundwater, and purchased water.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Source Water* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 3a: Pipes and Constructed Conveyances, Water Collection, and Intake (Malevolent Acts)

Asset Category: *Pipes and Constructed Conveyances, Water Collection, and Intake* **Examples of Assets in this Category:** Encompasses the infrastructure that collects and transports water from a source water to treatment or distribution facilities. Possible examples include holding facilities, intake structures and associated pumps and pipes, aqueducts, and other conveyances.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Pipes and Constructed Conveyances, Water Collection, and Intake* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[9]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Intentional Contamination of Finished Water	
☐ Intentional Contamination of Source Water	
☐ Other(s), enter below:	

[9] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Table 3b: Pipes and Constructed Conveyances, Water Collection, and Intake (Natural Hazards)

Asset Category: *Pipes and Constructed Conveyances, Water Collection, and Intake* **Examples of Assets in this Category:** Encompasses the infrastructure that collects and transports water from a source water to treatment or distribution facilities. Possible examples include holding facilities, intake structures and associated pumps and pipes, aqueducts, and other conveyances.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Pipes and Constructed Conveyances, Water Collection, and Intake* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 4a: Pretreatment and Treatment (Malevolent Acts)

Asset Category: *Pretreatment and Treatment* **Examples of Assets in this Category:** Encompasses all unit processes that a water system uses to ensure water meets regulatory public health and aesthetic standards prior to distribution to customers. Possible examples include sedimentation, filtration, disinfection, and chemical treatment. For the risk assessment, individual treatment processes at a facility may be grouped together and analyzed as a single asset if they have a similar risk profile.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Pretreatment and Treatment* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[10]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Intentional Contamination of Finished Water	

[10] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Asset Category: *Pretreatment and Treatment* **Examples of Assets in this Category:** Encompasses all unit processes that a water system uses to ensure water meets regulatory public health and aesthetic standards prior to distribution to customers. Possible examples include sedimentation, filtration, disinfection, and chemical treatment. For the risk assessment, individual treatment processes at a facility may be grouped together and analyzed as a single asset if they have a similar risk profile.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Pretreatment and Treatment* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Intentional Contamination of Source Water	
☐ Other(s), enter below:	

Table 4b: Pretreatment and Treatment (Natural Hazards)

Asset Category: *Pretreatment and Treatment* **Examples of Assets in this Category:** Encompasses all unit processes that a water system uses to ensure water meets regulatory public health and aesthetic standards prior to distribution to customers. Possible examples include sedimentation, filtration, disinfection, and chemical treatment. For the risk assessment, individual treatment processes at a facility may be grouped together and analyzed as a single asset if they have a similar risk profile.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Pretreatment and Treatment* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 5a: Storage and Distribution Facilities (Malevolent Acts)

Asset Category: *Storage and Distribution Facilities* **Examples of Assets in this Category:** Encompasses all infrastructure used to store water after treatment, maintain water quality, and distribute water to customers. Possible examples include residual disinfection, pumps, tanks, reservoirs, valves, pipes, and meters.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Storage and Distribution Facilities* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[11]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Intentional Contamination of Finished Water	
☐ Intentional Contamination of Source Water	
☐ Other(s), enter below:	

[11] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Table 5b: Storage and Distribution Facilities (Natural Hazards)

Asset Category: *Storage and Distribution Facilities* **Examples of Assets in this Category:** Encompasses all infrastructure used to store water after treatment, maintain water quality, and distribute water to customers. Possible examples include residual disinfection, pumps, tanks, reservoirs, valves, pipes, and meters.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Storage and Distribution Facilities* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 6a: Electronic, Computer, or Other Automated Systems (including the security of such systems) (Malevolent Acts)

Asset Category: *Electronic, Computer, or Other Automated Systems (including the security of such systems)*
Examples of Assets in this Category: Encompasses all treatment and distribution operational technology (OT) or process control systems, business enterprise information technology (IT) and communications systems (other than financial), and the processes used to secure such systems. Possible examples include the controls, monitors and other interfaces, plus related IT hardware and software and communications, used to control water collection, treatment, and distribution. Also includes IT hardware, software, and communications used in business enterprise operations. The assessment must account for the security of these systems (e.g., cybersecurity, information security).

Note: This table focuses on how specific malevolent acts may impact the cybersecurity and information security of electronic, computer, or other automated systems. In addition, CWSs should complete Table 11, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Electronic, Computer, or Other Automated Systems (including the security of such systems)* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[12]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Other(s), enter below:	

[12] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Table 6b: Electronic, Computer, or Other Automated Systems (including the security of such systems) (Natural Hazards)

Asset Category: *Electronic, Computer, or Other Automated Systems (including the security of such systems)*
Examples of Assets in this Category: Encompasses all treatment and distribution operational technology (OT) or process control systems, business enterprise information technology (IT) and communications systems (other than financial), and the processes used to secure such systems. Possible examples include the controls, monitors and other interfaces, plus related IT hardware and software and communications, used to control water collection, treatment, and distribution. Also includes IT hardware, software, and communications used in business enterprise operations. The assessment must account for the security of these systems (e.g., cybersecurity, information security).

Note: This table focuses on how specific natural hazards may impact the cybersecurity and information security of electronic, computer, or other automated systems. In addition, CWSs should complete Table 11, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Electronic, Computer, or Other Automated Systems (including the security of such systems)* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	

Asset Category: *Electronic, Computer, or Other Automated Systems (including the security of such systems)*
Examples of Assets in this Category: Encompasses all treatment and distribution operational technology (OT) or process control systems, business enterprise information technology (IT) and communications systems (other than financial), and the processes used to secure such systems. Possible examples include the controls, monitors and other interfaces, plus related IT hardware and software and communications, used to control water collection, treatment, and distribution. Also includes IT hardware, software, and communications used in business enterprise operations. The assessment must account for the security of these systems (e.g., cybersecurity, information security).

Note: This table focuses on how specific natural hazards may impact the cybersecurity and information security of electronic, computer, or other automated systems. In addition, CWSs should complete Table 11, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Electronic, Computer, or Other Automated Systems (including the security of such systems)* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 7a: Monitoring Practices (Malevolent Acts)[13]

Asset Category: *Monitoring Practices* **Examples of Assets in this Category:** Encompasses the processes and practices used to monitor source water and finished water quality, along with any monitoring systems not captured in other asset categories. Possible examples include sensors, laboratory resources, sampling capabilities, and data management equipment and systems that are implemented as part of a contamination warning system for a source water or distribution system.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Monitoring Practices* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[14]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Intentional Contamination of Finished Water	

[13] Monitoring associated with physical security should be addressed under Physical Barriers; monitoring associated with process controls and cybersecurity should be addressed under Electronic, Computer or Other Automated Systems; monitoring associated with financial systems should be addressed under Financial Infrastructure.

[14] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Asset Category: *Monitoring Practices* **Examples of Assets in this Category:** Encompasses the processes and practices used to monitor source water and finished water quality, along with any monitoring systems not captured in other asset categories. Possible examples include sensors, laboratory resources, sampling capabilities, and data management equipment and systems that are implemented as part of a contamination warning system for a source water or distribution system.	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Monitoring Practices* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Intentional Contamination of Source Water	
☐ Other(s), enter below:	

Table 7b: Monitoring Practices (Natural Hazards)[15]

Asset Category: *Monitoring Practices* **Examples of Assets in this Category:** Encompasses the processes and practices used to monitor source water and finished water quality, along with any monitoring systems not captured in other asset categories. Possible examples include sensors, laboratory resources, sampling capabilities, and data management equipment and systems that are implemented as part of a contamination warning system for a source water or distribution system.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Monitoring Practices* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	

[15] Monitoring associated with physical security should be addressed under Physical Barriers; monitoring associated with process controls and cybersecurity should be addressed under Electronic, Computer or Other Automated Systems; monitoring associated with financial systems should be addressed under Financial Infrastructure.

Asset Category: *Monitoring Practices* **Examples of Assets in this Category:** Encompasses the processes and practices used to monitor source water and finished water quality, along with any monitoring systems not captured in other asset categories. Possible examples include sensors, laboratory resources, sampling capabilities, and data management equipment and systems that are implemented as part of a contamination warning system for a source water or distribution system.	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Monitoring Practices* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Fire	
☐ Other(s), enter below:	

Table 8a: Financial Infrastructure (Malevolent Acts)

Asset Category: *Financial Infrastructure* **Examples of Assets in this Category:** Encompasses equipment and systems used to operate and manage CWS finances. Possible examples include billing, payment, and accounting systems, along with third parties used for these services. This asset category is not intended to address the financial "health" of the CWS (e.g., credit rating, debt-to-equity ratios).	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Financial Infrastructure* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[16]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Other(s), enter below:	

[16] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Table 8b: Financial Infrastructure (Natural Hazards)

Asset Category: *Financial Infrastructure* **Examples of Assets in this Category:** Encompasses equipment and systems used to operate and manage CWS finances. Possible examples include billing, payment, and accounting systems, along with third parties used for these services. This asset category is not intended to address the financial "health" of the CWS (e.g., credit rating, debt-to-equity ratios).	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Financial Infrastructure* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 9a: The Use, Storage, or Handing of Chemicals (Malevolent Acts)

Asset Category: *The Use, Storage, or Handling of Chemicals* **Examples of Assets in this Category:** Encompasses the chemicals and associated storage facilities and handling practices used for chemical disinfection and treatment. Assessments under this asset category should focus on the risk of uncontrolled release of a potentially dangerous chemical (e.g., chlorine).	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Use, Storage, or Handling of Chemicals* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[17]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Intentional Contamination of Finished Water	

[17] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Asset Category: *The Use, Storage, or Handling of Chemicals* **Examples of Assets in this Category:** Encompasses the chemicals and associated storage facilities and handling practices used for chemical disinfection and treatment. Assessments under this asset category should focus on the risk of uncontrolled release of a potentially dangerous chemical (e.g., chlorine).	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Use, Storage, or Handling of Chemicals* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Intentional Contamination of Source Water	
☐ Cyberattack	
☐ Other(s), enter below:	

Table 9b: The Use, Storage, or Handing of Chemicals (Natural Hazards)

Asset Category: *The Use, Storage, or Handling of Chemicals* **Examples of Assets in this Category:** Encompasses the chemicals and associated storage facilities and handling practices used for chemical disinfection and treatment. Assessments under this asset category should focus on the risk of uncontrolled release of a potentially dangerous chemical (e.g., chlorine).	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Use, Storage, or Handling of Chemicals* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 10a: The Operation and Maintenance of the System (Malevolent Acts)

Asset Category: *The Operation and Maintenance of the System* **Examples of Assets in this Category:** Encompasses critical processes required for operation and maintenance of the CWS that are not captured under other asset categories. Possible examples include equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like loss of utilities (e.g., power outages), loss of suppliers (e.g., interruption in chemical deliveries), and loss of key employees (e.g., disease outbreak or employee displacement).	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Operation and Maintenance of the System* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Cyberattack[18]	
☐ Assault on Utility – Physical	
☐ Theft or Diversion – Physical	
☐ Sabotage – Physical	
☐ Intentional Contamination of Finished Water	

[18] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against water systems in the United States. The EPA strongly recommends that your water system consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

Asset Category: *The Operation and Maintenance of the System* **Examples of Assets in this Category:** Encompasses critical processes required for operation and maintenance of the CWS that are not captured under other asset categories. Possible examples include equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like loss of utilities (e.g., power outages), loss of suppliers (e.g., interruption in chemical deliveries), and loss of key employees (e.g., disease outbreak or employee displacement).	
Malevolent Acts Select the malevolent acts in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a malevolent act in the left column as a significant risk to the *Operation and Maintenance of the System* asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Intentional Contamination of Source Water	
☐ Other(s), enter below:	

Table 10b: The Operation and Maintenance of the System (Natural Hazards)

Asset Category: *The Operation and Maintenance of the System* **Examples of Assets in this Category:** Encompasses critical processes required for operation and maintenance of the CWS that are not captured under other asset categories. Possible examples include equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like loss of utilities (e.g., power outages), loss of suppliers (e.g., interruption in chemical deliveries), and loss of key employees (e.g., disease outbreak or employee displacement).	
Natural Hazards Select the natural hazards in this column that pose a significant risk to this asset category at the CWS.	**Brief Description of Impacts** If you select a natural hazard in the left column as a significant risk to the *Operation and Maintenance of the System* asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
☐ Hurricane	
☐ Flood	
☐ Earthquake	
☐ Tornado	
☐ Ice storm	
☐ Fire	
☐ Other(s), enter below:	

Table 11: Checklist of Priority Cybersecurity Practices for Water Systems

	Question Does the CWS…	**Answer** Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
Reduce Exposure to Public-Facing Internet		
1.	Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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.*
Conduct Regular Cybersecurity Assessments		
2.	Conduct regular cybersecurity assessments?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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.*
3.	Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: Identify one role/position/title responsible for cybersecurity within the CWS. Whoever fills this role/position/title is then in charge of all CWS cybersecurity activities.*
Change Default Passwords Immediately		
4.	Change default passwords and require a minimum length for passwords?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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.*

	Question Does the CWS…	**Answer** Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
5.	Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access CWS/ OT/IT networks?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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.*
Conduct Inventory of OT/IT Assets		
6.	Maintain an updated inventory of all OT and IT network assets?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: Regularly review (no less than monthly) and maintain a list of all Operational Technology (OT) and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment. Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.*
7.	Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version.*
Develop and Exercise Cybersecurity Incident Response and Recovery Plans		
8.	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 reviewed, practiced, and updated?	☐ Yes Date of last IR plan review/update: ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: Develop, practice, review, and update an IR plan for cybersecurity incidents that could impact CWS operations. Participate in discussion-based (ex. TTX) and operations-based exercises (ex. Drill) to improve responses to potential cyber incidents.*

	Question Does the CWS…	**Answer** Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
9.	Have a written procedure for reporting cybersecurity incidents, including how and to whom? (e.g., phone call, internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, Water Information Sharing & Analysis Center - WaterISAC, cyber insurance provider)?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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 (see OW factsheet).*
Backup OT/IT Systems		
10.	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?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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.*
Reduce Exposure to Vulnerabilities		
11.	Patch or otherwise mitigate known vulnerabilities within the recommended time frame?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.*
12.	Require unique and separate credentials for users to access OT and IT networks and separate user and privileged (e.g., System Administrator) accounts?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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 and 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.*

	Question Does the CWS…	**Answer** Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
13.	Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.*
14.	Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: Terminate access immediately to accounts or networks upon a change in an individual's status making access unnecessary (i.e., retirement, change in position, etc.).*
Conduct Cybersecurity Awareness Training		
15.	Provide/conduct annual cybersecurity awareness training for all CWS personnel that covers basic cybersecurity concepts?	☐ Yes ☐ No ☐ In progress ☐ Not applicable *If "No", EPA recommends that the CWS take the following action: 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.*

Table 12: Countermeasures (Optional)[19]

Countermeasures (optional) List countermeasures in the left column the CWS could potentially implement to reduce risk from the malevolent acts and natural hazards that were selected.	Brief Description of Risk Reduction or Increased Resilience For each countermeasure, in the right column, describe how the countermeasure could reduce risk or increase resilience for CWS assets from malevolent acts or natural hazards that were selected in the analysis. A countermeasure may reduce risk across multiple malevolent acts, natural hazards, and asset categories.
1.	
2.	
3.	
4.	
5.	

[19] The assessment does not require a specific number of countermeasures. You may have fewer than five countermeasures or add more countermeasures on a separate sheet.

Change History

Please describe the changes made to this risk and resilience assessment since its original development, who made the changes, and on what date the changes were incorporated.

Name/Title:	Date:	Description of Change: