# Guidance on Risk and Resilience Assessments for Small Wastewater Utilities

## What is the Purpose of this Guidance?

This guidance will help small wastewater utilities conduct risk and resilience assessments (RRAs) of their facilities.

This guidance helps wastewater utilities assess the risk to their system from malevolent acts and natural hazards for the following asset categories, which align with relevant asset categories that community drinking water systems are required to address under America's Water Infrastructure Act (AWIA) Section 2013/Safe Drinking Water Act (SDWA) Section 1433: 1) physical barriers; 2) pipes and constructed conveyances, wastewater collection, and stormwater collection; 3) treatment; 4) storage and distribution facilities; 5) electronic, computer, or other automated systems (including the security of such systems); 6) monitoring practices; 7) financial infrastructure; 8) use, storage, or handing of chemicals; 9) operation and maintenance of the system.

This guidance does not address emergency response plans (ERPs). EPA has developed an ERP Template and Instructions for Wastewater Utilities to help develop ERPs. EPA recommends that wastewater utilities complete an ERP shortly after completing their RRA.

Further, this guidance does not cover all aspects of wastewater utility 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.

EPA recommends that wastewater utilities should review their RRA at least once every five years, and revise it as needed.

## Who Should Use this Guidance?

Small wastewater utilities serving fewer than 50,000 people that are interested in conducting RRAs and addressing threats from malevolent acts and natural hazards that could threaten wastewater utility service. For larger wastewater utilities, 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.

## What are Risk and Resilience in a Wastewater Utility?

Risk to critical infrastructure, including wastewater utilities, is a function of t**hreat likelihood, vulnerability,** and **consequence.**

- **Threat** can be a malevolent act (e.g.,a cyberattack or process sabotage), or a natural hazard (e.g. a flood or hurricane).
- **Threat likelihood** is the probability that a malevolent act will be carried out against a wastewater utility 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 wastewater utility would suffer significant adverse impacts.
- **Consequences** are the magnitude of loss that would ensue if a threat had an adverse impact against a wastewater utility. Consequences may include:
    - Economic loss to the wastewater utility from damage to CWS assets
    - Economic loss to a utility 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 a wastewater utility.

**Resilience** is the capability of a wastewater utility to maintain operations or recover quickly when a malevolent act or a natural hazard occurs.

**Countermeasures** are mitigation steps that a wastewater utility implements to reduce risk and increase resilience. They may include plans, equipment, and procedures.

## How Does a Wastewater Utility Assess Risk and Resilience?

**Tables 1a – 9b** in the *Risk and Resilience Assessment Checklist* (see fillable checklist beginning on page 1 or fillable Word checklist embedded on page iii) list the categories of wastewater utility assets. For all the tables (i.e., for all asset categories), do the following:

1. Select the **malevolent acts** from those listed that pose a significant risk to the asset category at the wastewater utility. You may write in malevolent acts not listed in the table.
    - Focus the selection of malevolent acts on those that can exploit vulnerabilities at the wastewater utility (e.g., known security gaps) and have the potential for significant economic, environmental, or public health consequences.
2. For each malevolent act that is identified as a significant risk, briefly describe how the act could impact the asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include major assets that might be damaged or disabled, wastewater service impacts or loss, and environmental and public health impacts, as applicable.
3. Select the **natural hazards** from those listed that may pose a significant risk to the asset category at the wastewater utility. You may write in natural hazards not listed in the table.
    - Focus the selection of natural hazards on those that may affect vulnerable wastewater utility infrastructure and have the potential for significant economic or environmental and public health consequences related to the wastewater utility.
4. For each natural hazard that identified as a significant risk, briefly describe, or provide examples of how the hazard could impact the asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include major assets that might be damaged or disabled, wastewater service impacts or loss, and environmental and public health impacts, as applicable.

**Table 10: Checklist of Priority Cybersecurity Practices for Wastewater Systems** can be used to evaluate cybersecurity best practices at a wastewater utility. 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 wastewater utility. 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 wastewater utility…" 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.

5. **OPTIONAL Table 11: Countermeasures** provides a table for you to identify countermeasures that the wastewater utility could potentially implement to reduce risk from the malevolent acts and natural hazards based on the information that you entered into tables 1a – 9b 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.

---

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

## Importance of Addressing Cybersecurity

Thoroughly addressing cybersecurity is essential in your wastewater utility's RRA. Cyberattacks are the highest-risk malevolent act carried out against wastewater utilities (and other critical infrastructure).

The risks from and resilience to cyberattacks against the asset categories in Tables 1a through 9b should be addressed where applicable (asset categories at wastewater utilities that do not involve electronic monitoring or control may not be at risk from cyberattacks). In addition, wastewater utilities should complete Table 10, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

If a wastewater utility 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.

## Complete the Wastewater Utility Risk and Resilience Assessment Checklist

EPA offers the wastewater utility *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.**

**Wastewater Utility Risk and Resilience Assessment Checklist**

# Wastewater Utility
# Risk and Resilience Assessment Checklist

## Enter Wastewater Utility Name Below:

_____

## Risk and Resilience Assessment

**Please fill in the information below.**

Facility Name (if applicable):

NPDES Permit No.:

Description of System:

Assessor Name(s):

Date of Assessment:

Assessment Notes:

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

| **Asset Category:** *Physical Barriers*<br>**Examples of Assets in this Category:** Encompasses physical security in place at the wastewater utility that may be damaged due to a malevolent act. Examples include, but are not limited to, 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**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a malevolent act in the left column as a significant risk to the *Physical Barriers* asset category, briefly describe in this column how the act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, 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, EPA recommends a wastewater utility assess the risks to and resilience of, physical barriers.

[7] Cyberattacks are the most prevalent and highest-risk malevolent act carried out against wastewater utilities in the United States. The EPA strongly recommends that your utility 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*<br>**Examples of Assets in this Category:** Encompasses physical security in place at the wastewater utility that may be damaged due to a natural hazard. Examples include, but are not limited to, 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**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a natural hazard in the left column as a significant risk to the *Physical Barriers* asset category, briefly describe in this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, 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, EPA recommends a wastewater utility assess the risks to and resilience of physical barriers.

## Table 2a: Pipes and Constructed Conveyances, Wastewater Collection, and Stormwater Collection (Malevolent Acts)

| **Asset Category:** *Pipes and Constructed Conveyances, Wastewater Collection, and Stormwater Collection*<br>**Examples of Assets in this Category:** Encompasses the infrastructure that collects and transports wastewater and stormwater from the source (e.g., homes, storm drains) to treatment facilities. Examples include, but are not limited to, pipes, manholes, tanks, lift stations, control structures, force mains, and associated pumps. | |
|---|---|
| **Malevolent Acts**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a malevolent act in the left column as a significant risk to the *Pipes and Constructed Conveyances, Wastewater Collection, and Stormwater Collection* asset category, briefly describe in this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Cyberattack[9] | |
| ☐ Assault on Utility – Physical | |
| ☐ Theft or Diversion – Physical | |
| ☐ Sabotage – Physical | |
| ☐ Other(s), enter below: | |

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

## Table 2b: Pipes and Constructed Conveyances, Wastewater Collection, and Stormwater Collection (Natural Hazards)

| **Asset Category:** *Pipes and Constructed Conveyances, Wastewater Collection, and Stormwater Collection*<br>**Examples of Assets in this Category:** Encompasses the infrastructure that collects and transports wastewater and stormwater from the source (e.g., homes, storm drains) to treatment facilities. Examples include, but are not limited to, pipes, manholes, tanks, lift stations, control structures, force mains, and associated pumps. | |
|---|---|
| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a natural hazard in the left column as a significant risk to the *Pipes and Constructed Conveyances, Wastewater Collection, and Stormwater Collection* asset category, briefly describe in this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 3a: Treatment (Malevolent Acts)

| **Asset Category:** *Treatment*<br>**Examples of Assets in this Category:** Encompasses all unit processes that a wastewater utility uses to ensure final effluent meets regulatory environmental standards prior to discharge to receiving waters. Examples include, but are not limited to, screening, sedimentation, aeration, clarification, and disinfection. 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**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a malevolent act in the left column as a significant risk to the *Treatment* asset category, briefly describe in this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Cyberattack[10] | |
| ☐ Assault on Utility – Physical | |
| ☐ Theft or Diversion – Physical | |
| ☐ Sabotage – Physical | |
| ☐ Other(s), enter below: | |

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

## Table 3b: Treatment (Natural Hazards)

| **Asset Category:** *Treatment*<br>**Examples of Assets in this Category:** Encompasses all unit processes that a wastewater utility uses to ensure final effluent meets regulatory environmental standards prior to discharge to receiving waters. Examples include, but are not limited to, screening, sedimentation, aeration, clarification, and disinfection. 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**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a natural hazard in the left column as a significant risk to the *Treatment* asset category, briefly describe in this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 4a: Storage and Distribution Facilities (Malevolent Acts)

| **Asset Category:** *Storage and Distribution Facilities*<br>**Examples of Assets in this Category:** Encompasses all infrastructure used to store excess influent (e.g., excess combined sewer flow) that would otherwise be bypassed to receiving waters and sewage lagoons. Examples include, but are not limited to, retention basins, pumps, valves, and pipes. | |
|---|---|
| **Malevolent Acts**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Cyberattack[11] | |
| ☐ Assault on Utility – Physical | |
| ☐ Theft or Diversion – Physical | |
| ☐ Sabotage – Physical | |
| ☐ Other(s), enter below: | |

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

## Table 4b: Storage and Distribution Facilities (Natural Hazards)

| **Asset Category:** *Storage and Distribution Facilities*<br>**Examples of Assets in this Category:** Encompasses all infrastructure used to store excess influent (e.g., excess combined sewer flow) that would otherwise be bypassed to receiving waters and sewage lagoons. Examples include, but are not limited to, retention basins, pumps, valves, and pipes. | |
|---|---|
| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 5a: 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 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. Examples include, but are not limited to, the sensors, controls, monitors and other interfaces, as well as related IT hardware and software and communications used to control wastewater collection, treatment, and discharge to receiving waters. 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, wastewater utilities should complete Table 10, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

| **Malevolent Acts**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, 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 wastewater utilities in the United States. The EPA strongly recommends that your utility consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

## Table 5b: 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 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. Examples include, but are not limited to, the sensors, controls, monitors and other interfaces, as well as related IT hardware and software and communications used to control wastewater collection, treatment, and discharge to receiving waters. 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, wastewater utilities should complete Table 10, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, 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 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. Examples include, but are not limited to, the sensors, controls, monitors and other interfaces, as well as related IT hardware and software and communications used to control wastewater collection, treatment, and discharge to receiving waters. 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, wastewater utilities should complete Table 10, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
|---|---|
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 6a: Monitoring Practices (Malevolent Acts)[13]

| **Asset Category:** *Monitoring Practices*<br>**Examples of Assets in this Category:** Encompasses the processes and practices used to monitor the wastewater treatment process and final effluent quality, along with any monitoring systems not captured in other asset categories. Examples include, but are not limited to, sensors, laboratory resources, sampling capabilities, and data management equipment and systems. | |
|---|---|
| **Malevolent Acts**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a malevolent act in the left column as a significant risk to the *Monitoring Practices* asset category, briefly describe in this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Cyberattack[14] | |
| ☐ Assault on Utility – Physical | |
| ☐ Theft or Diversion – Physical | |
| ☐ Sabotage – Physical | |
| ☐ Other(s), enter below: | |

[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 wastewater utilities in the United States. The EPA strongly recommends that your utility consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

## Table 6b: Monitoring Practices (Natural Hazards)[15]

| **Asset Category:** *Monitoring Practices*<br>**Examples of Assets in this Category:** Encompasses the processes and practices used to monitor the wastewater treatment process and final effluent quality, along with any monitoring systems not captured in other asset categories. Examples include, but are not limited to, sensors, laboratory resources, sampling capabilities, and data management equipment and systems. | |
|---|---|
| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a natural hazard in the left column as a significant risk to the *Monitoring Practices* asset category, briefly describe in this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

[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.

## Table 7a: Financial Infrastructure (Malevolent Acts)

| **Asset Category:** *Financial Infrastructure*<br>**Examples of Assets in this Category:** Encompasses equipment and systems used to operate and manage utility finances. Examples include, but are not limited to, 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 wastewater utility (e.g., credit rating, debt-to-equity ratios). | |
|---|---|
| **Malevolent Acts**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a malevolent act in the left column as a significant risk to the *Financial Infrastructure* asset category, briefly describe in this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, 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 wastewater utilities in the United States. The EPA strongly recommends that your utility consider assessing the threat of a cyberattack for as many asset categories as deemed relevant by your utility.

## Table 7b: Financial Infrastructure (Natural Hazards)

| **Asset Category:** *Financial Infrastructure*<br>**Examples of Assets in this Category:** Encompasses equipment and systems used to operate and manage utility finances. Examples include, but are not limited to, 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 wastewater utility (e.g., credit rating, debt-to-equity ratios). | |
|---|---|
| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>If you select a natural hazard in the left column as a significant risk to the *Financial Infrastructure* asset category, briefly describe in this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 8a: Use, Storage, or Handing of Chemicals (Malevolent Acts)

| **Asset Category:** *Use, Storage, or Handling of Chemicals*<br>**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 chemicals like chlorine or other disinfectants and treatment chemicals. | |
|---|---|
| **Malevolent Acts**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Cyberattack[17] | |
| ☐ Assault on Utility – Physical | |
| ☐ Theft or Diversion – Physical | |
| ☐ Sabotage – Physical | |
| ☐ Other(s), enter below: | |

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

## Table 8b: Use, Storage, or Handing of Chemicals (Natural Hazards)

| **Asset Category:** *Use, Storage, or Handling of Chemicals*<br>**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 chemicals like chlorine or other disinfectants and treatment chemicals. | |
|---|---|
| **Natural Hazards**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 9a: Operation and Maintenance of the System (Malevolent Acts)

| **Asset Category:** *Operation and Maintenance of the System*<br>**Examples of Assets in this Category:** Encompasses critical processes required and key-components for operation and maintenance of the wastewater utility that are not captured under other asset categories. Examples include, but are not limited to, 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**<br>Select the malevolent acts in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the malevolent act could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Cyberattack[18] | |
| ☐ Assault on Utility – Physical | |
| ☐ Theft or Diversion – Physical | |
| ☐ Sabotage – Physical | |
| ☐ Other(s), enter below: | |

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

## Table 9b: Operation and Maintenance of the System (Natural Hazards)

| **Asset Category:** *Operation and Maintenance of the System*<br>**Examples of Assets in this Category:** Encompasses critical processes and key-components required for operation and maintenance of the wastewater utility that are not captured under other asset categories. Examples include, but are not limited to, 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**<br>Select the natural hazards in this column that pose a significant risk to this asset category at the wastewater utility. | **Brief Description of Impacts**<br>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 this column how the natural hazard could impact this asset category at the wastewater utility, especially as the impact relates to existing vulnerabilities at the utility. Include effects on major assets, wastewater service, environment, and public health, as applicable. |
| ☐ Hurricane | |
| ☐ Flood | |
| ☐ Earthquake | |
| ☐ Tornado | |
| ☐ Ice storm | |
| ☐ Fire | |
| ☐ Other(s), enter below: | |

## Table 10: Checklist of Priority Cybersecurity Practices for Wastewater Systems

| | **Question**<br>Does the wastewater utility… | **Answer**<br>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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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 utility? | ☐ Yes<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility take the following action: Identify one role/position/title responsible for cybersecurity within the utility. Whoever fills this role/position/title is then in charge of all utility cybersecurity activities.* |
| **Change Default Passwords Immediately** | | |
| 4. | Change default passwords and require a minimum length for passwords? | ☐ Yes<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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**<br>Does the wastewater utility… | **Answer**<br>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 utility/OT/IT networks? | ☐ Yes<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>Date of last IR plan review/update:<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility take the following action: Develop, practice, review, and update an IR plan for cybersecurity incidents that could impact utility operations. Participate in discussion-based (ex. TTX) and operations-based exercises (ex. Drill) to improve responses to potential cyber incidents.* |

| | **Question**<br>Does the wastewater utility… | **Answer**<br>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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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:*<br>*3) Keep three copies: one primary and two backups;*<br>*2) Keep the backups on two different media types;*<br>*1) Store one copy offsite.* |
| **Reduce Exposure to Vulnerabilities** | | |
| 11. | Patch or otherwise mitigate known vulnerabilities within the recommended time frame? | ☐ Yes<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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**<br>Does the wastewater utility… | **Answer**<br>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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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 utility personnel that covers basic cybersecurity concepts? | ☐ Yes<br>☐ No<br>☐ In progress<br>☐ Not applicable<br><br>*If "No", EPA recommends that the utility 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 11: Countermeasures (Optional)[19]

| Countermeasures (optional)<br>List countermeasures in the left column the wastewater utility could potentially implement to reduce risk from the malevolent acts and natural hazards that were selected. | Brief Description of Risk Reduction or Increased Resilience<br>For each countermeasure listed in the left column, describe in this column how the countermeasure could reduce risk or increase resilience for wastewater utility 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: |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |