United States
Environmental Protection
Agency

Baseline Information on Malevolent Acts for Community Water Systems

Version 3.0

Office of Water (MC 140) EPA/817/R-24/001 May 2024

Version History for Baseline Information on Malevolent Acts for Community Water Systems

Version	Publication Date	Significant Changes from Prior Version
1.0	August 1, 2019	• Original publication
2.0	February 2021	• Increased the default threat likelihood value to 1.0 for cyberattack on business enterprise systems and cyberattack on process control systems.
3.0	May 2024	• Replaced most point estimates of default threat likelihood with order of magnitude ranges. • Eliminated accidental contamination of source and finished water as malevolent act threat categories. • Revised factors potentially impacting threat likelihood. • Eliminated default threat likelihood values for wastewater. • Combined cyberattacks on business enterprise systems and process control systems into a single category of cyberattack.

Disclaimer

The Water Infrastructure and Cyber Resilience Division of the Office of Ground Water and Drinking Water has reviewed and approved this document for publication. This document does not impose legally binding requirements on any party. The information in this document is intended solely to recommend or suggest and does not establish any requirements. Neither the United States Government nor any of its employees, contractors or their employees make any warranty, expressed or implied, or assume any legal liability or responsibility for any third party's use of any information, product, or process discussed in this document, or represent that its use by such party would not infringe on privately owned rights. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Questions and comments concerning this document should be addressed to WQ_SRS@epa.gov or the following contact:

Dan Schmelling
U.S. EPA Water Infrastructure and Cyber Resilience Division
1200 Pennsylvania Ave, NW
Mail Code 4608T Washington, DC 20460
(202) 557-0683
Schmelling.Dan@epa.gov

Table of Contents

List of Figures

List of Tables

Abbreviations

ASCE	American Society of Civil Engineers
AWIA	America's Water Infrastructure Act of 2018
AWWA	American Water Works Association
CISA	Cybersecurity and Infrastructure Security Agency
CWS	Community Water System
DHS	U.S. Department of Homeland Security
EPA	U.S. Environmental Protection Agency
ERP	Emergency Response Plan
FBI	Federal Bureau of Investigation
IT	Information Technology
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OT	Operational Technology
SDWA	Safe Drinking Water Act
WaterISAC	Water Information Sharing and Analysis Center

Introduction

Clean and safe water is essential to human health and the nation's economy. Public water systems, like other critical infrastructure, face an array of threats from both natural hazards (e.g., floods, hurricanes) and malevolent acts (e.g., cyberattacks, contamination). This guidance document can help public water system owners and operators to assess the threat that certain malevolent acts pose to their systems and to identify steps that may reduce their risk.

As discussed in Section 2, assessing threats is a critical step in an "all-hazards" approach to risk management, which also involves:

- Evaluating and mitigating the vulnerabilities of critical assets, and
- Understanding and reducing the potential consequences of incidents that may occur.

Pursuant to the requirements in Sec. 2013 of America's Water Infrastructure Act (AWIA) of 2018, which amended Sec. 1433 of the Safe Drinking Water Act (SDWA), the U.S. Environmental Protection Agency (EPA), in consultation with federal, state, and local government partners, developed this guidance document with baseline information on malevolent acts relevant to community water systems (CWSs).[1]

The information provided in this document is not a threat analysis for a specific water system. Due to significant variability in assets, operations, system design, and other characteristics that influence the risk presented by malevolent acts, some information in this document may not be relevant to certain water systems. Default threat likelihood ranges are offered only as a starting point for water system owners and operators to consider when estimating the probability of malevolent acts as part of a risk and resilience assessment.[2] When conducting site-specific assessments, analysts may determine that lower or higher threat likelihood values are appropriate. The process water systems go through to assess threats should account for their unique situations, which cannot be reflected in the baseline values in this guidance.

This document contains the following sections:

- **Section 1: AWIA Requirements** – Provides an overview of AWIA requirements pertaining to risk and resilience assessments, emergency response plans (ERPs), and baseline threat information.
- **Section 2: Assessing Risk and Resilience** – Describes the basic elements of risk and resilience assessments for CWSs.
- **Section 3: Asset Categories** – Defines physical and cyber elements that CWSs are required to evaluate in conducting risk and resilience assessments under AWIA.
- **Section 4: Threat Categories and Default Likelihoods for Malevolent Acts** – Describes threat categories for malevolent acts relevant to CWSs and default threat likelihood ranges.
- **Section 5: Estimating Threat Likelihood and Deterrence Factors** – Presents the basis for default threat likelihood ranges and lists factors that may impact threat likelihood estimates by deterring threat actors.

[1] A Community Water System (CWS) is a public water system that supplies water to the same population year-round.

[2] In accordance with AWIA, natural hazards and dependency/proximity threats are outside the scope of this document but should be included in a risk and resilience assessment.

Section 1: AWIA Requirements

1.1 Risk Assessments and Emergency Response Plans

America's Water Infrastructure Act (AWIA) *of 2018* was enacted as Public Law No: 115-270 on October 23, 2018 (BILLS-115s3021enr.pdf (congress.gov). This law mandated that all CWSs serving more than 3,300 people conduct risk and resilience assessments that consider risks to the water system from malevolent acts and natural hazards. The statute specified water treatment and distribution system components that the assessment must include (discussed in Section 3).

Under AWIA, CWSs were also required to prepare or revise an emergency response plan (ERP) that incorporated the findings of the risk and resilience assessment. The statute listed areas of water system security and operations that the ERP must include (see America's Water Infrastructure Act Section 2013: Risk and Resilience Assessments and Emergency Response Plans | US EPA for additional information). Further, the law established deadlines for CWSs to certify the completion of the initial risk and resilience assessment and ERP to EPA. Final dates for certifying the first risk and resilience assessments ranged from March 31, 2020, to June 30, 2021, depending on CWS size, and the deadline for certifying the ERPs followed by six months.

AWIA requires CWSs to review their risk and resilience assessments at least once every five years to determine whether the assessment should be revised. After completing the review, CWSs must certify to EPA that they reviewed and, if applicable, revised the assessment. CWSs must then incorporate any revisions from their risk and resilience assessments into their ERPs, and must certify to EPA that they reviewed and, if necessary, revised the ERP not later than six months after the applicable deadline for certifying assessments. Upcoming due dates for certifying the review and revision of risk and resilience assessments and ERPs are shown in **Table 1**, below.

Table 1: Upcoming Certification Deadlines by CWS Size for Review of AWIA Risk and Resilience Assessments and ERPs

Population Served*	Risk Assessment Review Certification Deadlines	Emergency Response Plan** Review Certification Deadlines
≥100,000	March 31, 2025	September 30, 2025
50,000-99,999	December 21, 2025	June 30, 2026
3,301-49,999	June 30, 2026	December 30, 2026

**When determining population served, wholesale CWSs (i.e., CWSs that sell water to other water systems) should include both their retail population served and the population served by all consecutive water systems.*

***ERP certifications are due no later than six months from the date the risk assessment is certified to EPA. The ERP due dates shown are based on a CWS certifying a risk assessment on the final due date.*

1.2 Baseline Information on Malevolent Acts

To assist CWSs with identifying threats to be considered in risk and resilience assessments, AWIA directed EPA to provide baseline information on malevolent acts that are relevant to CWSs, including acts that may either:

- Substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or
- Otherwise present significant public health or economic concerns to the community served by the system.

EPA published *Baseline Information on Malevolent Acts for Community Water Systems* on August 1, 2019 (the AWIA publication deadline). This document addressed the assessment of threats related to malevolent acts at water systems, as required by AWIA, and provided an overview of how this information could be used in the risk assessment process. In response to public comment and new information, EPA published Version 2.0 of this document, which revised the default threat likelihood values for cyberattacks on business enterprise systems and process control systems, in February 2021.

After consultation with government and water sector partners, EPA is issuing the current version of this document (Version 3.0) to assist CWSs with reviewing and, as needed, revising their risk and resilience assessments in anticipation of the upcoming certification deadlines. See the "Version History" table on page i for a list of significant changes between Versions 2.0 and 3.0.

Section 2: Assessing Risk and Resilience

The American Water Works Association (AWWA) Standard, J100-21, *Risk and Resilience Management of Water and Wastewater Systems*[3], (hereinafter, "the J100 Standard") defines risk as follows:

> *Risk:* A function of (1) consequences, (2) hazard frequency or threat likelihood, and (3) vulnerability, which, with point estimates, is the product of these three terms. It is the expected value of the consequences of an initiating event weighted by the likelihood of the event's occurrence and the likelihood that the event will result in the consequences, given that it occurs. Risk is based on identified events or event scenarios.

The J100 Standard defines the component terms of risk as follows:

> Risk = Threat x Vulnerability x Consequence
>
> *Threat:* A man-made, natural, dependency or proximity incident with the potential to cause harm. In malevolent risk analysis, threat is based on the analysis of the intent and capability of an adversary (whether insider or outsider) to undertake actions that would be detrimental to an asset. *Threat likelihood* is the probability that an undesirable event will occur in a specified period of time, normally one year.
>
> *Vulnerability:* The effectiveness of the countermeasures to protect an asset from a defined threat. Therefore, it is the inherent state of a system (e.g., physical, technical, organizational, cultural) that can be exploited by an adversary or impacted by a natural or dependency/proximity hazard to cause harm or damage. *Vulnerability estimate* is the conditional probability that a specific threat, given that it occurs, will cause the specific estimated consequences to the asset. For malevolent threats, it may be interpreted as the likelihood of an adversary's success, given the threat occurs.
>
> *Consequence:* Human, financial and property losses, environmental damages, and lifeline service interruptions for the immediate, short- and long-term effects of a threat on an asset (threat-asset pair). These effects include losses suffered by the owner of the asset and losses suffered by the community

[3] ANSI/AWWA J100-21, *Risk and Resilience Management of Water and Wastewater Systems*, AWWA Standard, effective May 1, 2021, available at https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/88116441.

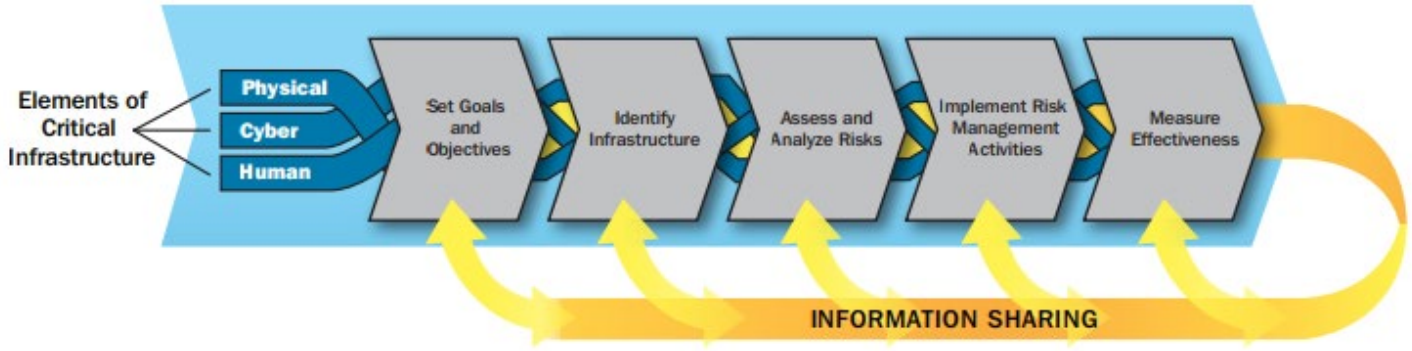
served by that asset, respectively.

Risk and resilience assessments identify the threats that present the highest risks to a water system's critical assets, systems, and networks. A risk assessment for a water system accounts for threats to source water (ground and surface), intake structures, treatment and distribution systems, operations, and business enterprise systems. It also considers risks posed to the surrounding community related to attacks on the water system. An effective risk and resilience assessment can facilitate the development of a prioritized plan for security upgrades, modifications of operational procedures, and policy changes to mitigate risks to and enhance the resilience of a water system's critical assets.

This document presents an overview of the baseline threat likelihood posed by malevolent acts to CWSs, which analysts may consider when conducting risk and resilience assessments under AWIA. ("Baseline" in this context is an ongoing level, which may be elevated situationally.) CWSs may select any appropriate risk assessment standard, methodology, or tool for assistance in meeting the requirements of AWIA. Regardless of the use of any standard, methodology or tool, CWSs are responsible for ensuring that their risk and resilience assessments and ERPs fully address all applicable AWIA requirements.

As described in the 2013 *National Infrastructure Protection Plan* (NIPP), *Critical Infrastructure Risk Management Framework*[4], the assessment of risks is one component of an overall risk management framework, which is shown in **Figure 1** (from Figure 3 of the 2013 NIPP). The nature and extent of the risk assessment will differ among water systems based on multiple factors, including the water system size and population served, water sources, and infrastructure, including treatment and distribution systems. The results of the risk assessment should be incorporated into an overall risk management plan, such as the approach shown in **Table 2**. With a risk management plan, water systems can use the results of the risk and resilience assessment to maximize short- and long-term risk reduction and resilience with available resources.

Figure 1: Critical Infrastructure Risk Management Framework



[4] *National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience,* U.S. Department of Homeland Security, available at https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

Table 2: Approach to Risk and Resilience Management

Step	Purpose
1. Set Goals and Objectives	Define specific outcomes, conditions, end points, or performance targets that collectively describe an effective and desired risk management posture.
2. Identify Infrastructure	Identify assets, systems, and networks that contribute to critical functionality and collect information pertinent to risk management, including analysis of dependencies and interdependencies.
3. Assess and Analyze Risk	Evaluate the risk, taking into consideration the potential direct and indirect consequences of an incident, known vulnerabilities to various potential threats or hazards, and general or specific threat information.
4. Implement Risk Management Activities	Make decisions and implement risk management approaches to control, accept, transfer, or avoid risks. Approaches can include prevention, protection, mitigation, response, and recovery activities.
5. Measure Effectiveness	Use metrics and other evaluation procedures to measure progress and assess the effectiveness of efforts to secure and strengthen the resilience of critical infrastructure.

Section 3: Asset Categories

AWIA requires the assessment of risks from, and resilience to, malevolent acts and natural hazards to include the asset categories listed in **Table 3**.[5,6] The EPA examples for each of the asset categories are offered as guidance only and may not apply to all CWSs. Each CWS should identify the critical assets to be assessed under AWIA based on existing design, infrastructure, and operations.

Table 3: AWIA-Identified Assets

Asset Category	EPA Examples
Pipes and constructed conveyances, water collection, and intake	Encompasses the infrastructure that collects and transports water from a source to treatment or distribution facilities. Possible examples include holding facilities, intake structures and associated pumps and pipes, aqueducts, and other conveyances.

[5] Per AWIA, the risk and resilience assessment may also include an evaluation of the capital and operational needs for risk and resilience management for the system.

[6] See section 1433(a)(1)(A) of the Safe Drinking Water Act as amended by AWIA.

Asset Category	EPA Examples
Physical barriers	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.[7]
Source water	Encompasses all sources that supply water to a CWS. Possible examples include rivers, streams, lakes, source water reservoirs, groundwater, and purchased water.
Pretreatment and treatment	Encompasses all unit processes that a CWS 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.
Storage and distribution facilities	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.
Electronic, computer, or other automated systems (including the security of such systems)	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 sensors, 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).

[7] 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. In this case, a CWS may consider increased risks to other system assets, along with economic impacts, if physical barriers were compromised.

Asset Category	EPA Examples
Monitoring practices	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. An example is a contamination warning system for the source water or distribution system.[8] This category may also include energy management systems.
Financial infrastructure	Encompasses equipment and systems used to operate and manage utility 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 water utility (e.g., credit rating, debt-to-equity ratios).
The use, storage, or handling of chemicals	Encompasses the chemicals and associated storage facilities and handling practices used for chemical disinfection and treatment. Assessments under this asset category should focus where applicable on the risk of uncontrolled release of a potentially dangerous chemical like chlorine.
The operation and maintenance of the system	Encompasses critical processes required for operation and maintenance of the water system that are not captured under other asset categories, including equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like the loss of utilities (e.g., power outage), loss of suppliers (e.g., interruption in chemical delivery), and loss of key employees (e.g., disease outbreak or employee displacement).

[8] 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.*

Section 4: Threat Categories and Default Likelihoods for Malevolent Acts

This section provides baseline information on malevolent acts of relevance to CWSs.

4.1 Threat Categories

The J100 Standard includes series of reference threats for malevolent acts, as well as natural hazards and dependency and proximity threats. For purposes of simplification, EPA has grouped the malevolent act reference threats into the categories shown in **Table 4**. These threat categories encompass actions that could be taken by a malevolent actor to either (1) substantially disrupt the ability of a system to provide a safe and reliable supply of drinking water, or (2) cause significant public health or economic impacts in the community served by the CWS. EPA recommends that CWSs consider this information when conducting risk and resilience assessments.

Table 4: EPA Threat Categories for Malevolent Acts

EPA Threat Category	J100 Standard Reference Threats
Assault on Utility – Physical	Aircraft: (A1) Helicopter, (A2) Small plane, (A3) Regional jet, (A4) Large jet Assault Team: (AT1) 1 Assailant, (AT2) 2-4 Assailants, (AT3) 5-8 Assailants, (AT4) 9-16 Assailants Maritime: (M1) Small boat, (M2) Fast boat, (M3) Barge, (M4) Deep draft ship Vehicle Borne Bomb: (V1) Car, (V2) Van, (V3) Midsize truck, (V4) Large truck (18-wheeler)
Intentional Contamination of Finished Water	C(B) Biotoxin, C(C) Chemical, C(S) Explosive, C(P) Pathogen, C(R) Radionuclide
Theft or Diversion – Physical	T(PI) Physical-insider, T(PU) Physical-outsider
Cyber	(CI) Cyberattack
Directed/Sabotage – Physical	S(PI) Physical-insider, S(PU) Physical-outsider, AS – Active shooter
Intentional Contamination of Source Water	Intentional contamination of source water is not a J100 Standard reference threat. EPA has included it as a threat category here based on prior recognition as a potential target of attack[9] and distinct threat characteristics (e.g., ease of access). The contaminant types listed as reference threats for *Intentional Contamination of Finished Water* also apply to this threat category.

[9] https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf

The grouping of reference threats into the threat categories in **Table 4** is offered as a streamlining approach for CWSs with more limited resources to conduct risk and resilience assessments. Further, as discussed in Section 4.3, data available to EPA are not sufficient to recommend different default threat likelihood values for reference threats within a given threat category. This approach can facilitate risk and resilience assessments to identify threats that present the highest risk to mission critical functions and, therefore, where security resources should be invested.

When supported by necessary resources and data, however, a risk and resilience assessment for individual reference threats from the J100 Standard can account for differences in actual threat likelihood values within a given Table 4 threat category, such as the following examples:

- Assault on Utility-Physical: attack by an individual assailant has an expected higher threat likelihood than attack by a large team.
- Intentional Contamination of Finished or Source Water: the expected threat likelihood for contamination with materials that are more readily available, such as toxic chemicals, is higher than contamination with materials that are tightly controlled, such as a radionuclide.

4.2 Estimating Threat Likelihood

As stated in Section 2, the J100 Standard defines *threat likelihood* as the probability (a value between 0 and 1) that an undesirable event (e.g., a malevolent act directed against the water system) will occur in a period of one year. Malevolent acts may be carried out by terrorists (international or domestic), criminals, hostile water system customers, contractors, or employees. No comprehensive database exists to provide an authoritative basis to estimate the probability of a water system being victimized by a malevolent act. Instead, the J100 Standard identifies two methods to estimate threat likelihood for malevolent acts: (1) *The Proxy Method for Estimation of Terrorist Threat Likelihood* (the Proxy method) and (2) the "best estimate."

The Proxy method entails six steps that assess a terrorist selecting (1) the country, (2) the metropolitan region, (3) the facility type, and (4) the specific utility to attack, then adjusts for (5) the likelihood of pre-attack detection and interdiction (which considers factors like the number of people involved in and the logistical difficulty of executing the attack), and (6) the selection of a specific threat-asset pair, which depends on the likelihood of a successful attack (the perceived vulnerability of the target), the potential for detection and interdiction before initiating the attack, and the expected consequences (e.g., causalities and economic disruption).

Alternatively, for the "best estimate" approach, analysts must rely on available information pertaining to the threat and facility asset, which may include the following:

- Historical data (e.g., prior frequency of the malevolent act) and knowledge of the community, particularly for certain malevolent acts like theft;
- Threat information from federal, state, and local intelligence, homeland security, and law enforcement agencies; and
- Knowledge of facility characteristics that may deter a malevolent actor.

4.3 Default Threat Likelihood Ranges

To assist CWSs with conducting risk and resilience assessments under AWIA, EPA is providing a range of default threat likelihood values for each of the threat categories in **Table 4**. These default values reflect a best estimate approach and are based on observations of publicly reported incidents at water systems in the United States. They are general, order-of-magnitude estimates that are intended to serve as a starting point for risk and resilience assessments. They are not a threat level for a specific water system. EPA recommends that CWSs consider the applicability of the default values to their facilities and develop site-specific threat likelihood estimates as needed.

Table 5: Default Threat Likelihood Ranges for Malevolent Act Threat Categories

Threat Likelihood Level	Default Threat Likelihood Range	Malevolent Act Threat Categories
Low	10^{-6} – 10^{-5}	Assault on utility – physical* Intentional contamination of source water Intentional contamination of finished water
Medium	0.01 – 0.1	Directed/Sabotage – physical Theft or diversion – physical**
High	1	Cyberattack

**Does not include routine crime that occurs in a community that may affect utility employees.*

***This threat likelihood range applies only to a major incident of physical theft or diversion of critical resources, equipment, supplies, or infrastructure materials with the potential to disrupt the operations of a water system. It matches the range assigned to Directed/Sabotage-physical because both categories involve physical acts against water system infrastructure or resources that may disrupt operations.*

The default threat likelihood ranges for the different threat categories in **Table 5** can allow for a simplified risk assessment for water systems that lack the resources to conduct the assessment on individual reference threats as described in the J100 Standard. As noted, these threat levels, when combined with estimates for the vulnerability and consequences associated with assets, can support an analyst in determining the threat-asset pairs that are the highest risks to water system operations. This information can help guide decisions on investments in mitigation strategies to reduce risk and build resilience.

The values in **Table 5** reflect observations of how regularly different types of security incidents have been reported by water systems nationally. Where analysts lack the information necessary for an accurate point estimate of the threat likelihood for a malevolent act at a particular facility, they may follow the best estimate approach used in this document, which characterizes malevolent acts as occurring:

- Frequently (i.e., “high”) (e.g., cyberattacks),
- Infrequently but are regularly reported by water systems or other critical infrastructure facilities (i.e., “medium”) (e.g., major theft that could impact operations, sabotage), or
- Rarely, if ever, reported by water systems (i.e., “low”) (e.g., intentional contamination, armed assaults on a facility).

Analysts that use the approach shown in **Table 5** may either determine a specific threat likelihood value from the suggested range or may conduct the analysis across the value range (e.g., analyze a high and low value) to reflect uncertainty in the estimate. The section that follows suggests “deterrence factors” that analysts may consider for assigning a higher or lower threat likelihood value to a threat category at a specific water system.

Section 5. Estimating Threat Likelihood and Deterrence Factors

When making a best estimate for the probability that an assailant will execute a certain malevolent act against a particular asset at a water system (i.e., the threat likelihood), analysts should consider factors that impact the "attractiveness" of the asset to an assailant. Consistent with step 6 of the Proxy Method from the J100 Standard, these factors may include the following asset qualities as perceived by an assailant prior to executing an attack:

- **Assessed vulnerability.** The likelihood as assessed by an assailant that the attack will achieve the intended consequences, which depends on visible security features of both the asset and the facility that are known or can be discovered by the assailant prior to the attack.
- **Risk of interdiction prior to initiation.** The risk that the logistics of the attack (e.g., number of people involved, difficulty of execution) would attract the attention of authorities and lead to detection and interdiction prior to initiating the attack.
- **Expected consequences.** The expected impact of the attack from the assailant's perspective, which could include human health or economic impacts, fomenting terror in a population, etc.

In the sections that follow, these facility qualities that may impact threat likelihood are referred to as "threat deterrence factors" to imply that they may to some degree deter an assailant from executing a malevolent act against a particular asset or facility. Many of these threat deterrence factors, however, are also important considerations in the estimation of "vulnerability" or "consequence" when assessing risk (discussed in Section 2). Accordingly, analysts should determine how to account for these factors in each component of risk when conducting a risk assessment.

5.1 Deterrence Factors for Threat Likelihood That Apply to Multiple Threat Categories

Table 6 presents threat deterrence factors that apply to multiple threat categories. These factors can be indicators of the general threat environment for a water system or facility. They may overlap and should be evaluated with threat deterrence factors for individual threat categories, discussed in Section 5.2, when making a site-specific threat likelihood estimate. Responses to questions for threat deterrence factors can also identify areas for consideration of security enhancements.

Available data are insufficient to provide a method for quantifying threat likelihood values based on responses to threat deterrence factor questions. Analysts should assess responses qualitatively and holistically in combination with site-specific knowledge, such as threat and incident history, security improvements, and available law enforcement and intelligence information to make best estimates of threat likelihood values at a CWS.

Table 6: General Threat Deterrence Factors

Factor	Impact on Threat Deterrence	Analyst Notes
1. Does the water system serve a major population center or prominent facility?	Water systems that serve large population centers or prominent facilities (e.g., large government installations) may be more attractive to an assailant due to higher expected consequences.	

Factor	Impact on Threat Deterrence	Analyst Notes
2. Does the water system infrastructure display strong visible physical security features (e.g., fencing, lighting, clear setbacks, guards, locked windows, grates, doors, and other access points, video cameras)?	The presence of visible physical security features can deter an assailant by decreasing the assessed vulnerability.	
3. Are there visible points in the water system infrastructure or operations where an attack could achieve complete disruption of the capability to supply safe drinking water?	A single point of failure (e.g., single source of water, single water storage tank) for water system operations that is visible to an assailant may increase the likelihood of an attack at that point due to higher expected consequences.	
4. Does the water system follow protocols for deescalating conflicts with disgruntled or hostile customers and employees?	A water system that proactively resolves complaints and deescalates conflicts may reduce like likelihood of being targeted for sabotage or other malevolent acts by hostile customers or employees.	
5. Are non-employees with access to water system facilities properly vetted?	Rigorous background checks of third parties with access to facilities or systems (e.g., contractors, vendors, IT service providers) prior to authorizing access may reduce the likelihood of being targeted for theft or sabotage.	
6. Do organizations with extremist political, social, or other ideologies operate in the vicinity of the water system?	Proximity to extremist organizations may increase the likelihood of the water system being targeted for malevolent acts (e.g., sabotage, contamination). Intelligence and law enforcement information on the capabilities and intent of an organization should be evaluated.	

5.2 Factors for Estimating Threat Likelihood That Apply to Individual Threat Categories

Tables 7 - 12 (for individual threat categories) presented below include the following:

- Corresponding reference threats from the J100 Standard,
- Rationale for the EPA default threat likelihood range,
- Threat deterrence factors for the individual threat category, and
- Publicly available resources for additional information.

See Section 5.1 regarding the use of threat deterrence factors in making best estimates of threat likelihood values.

Table 7a: Threat Category: Assault on Utility – Physical

Threat Category Definition: *A physical assault on water system infrastructure or staff with the intent of disabling infrastructure and/or terrorizing staff. Does not include routine crime that occurs in a community and may involve utility employees. Does not include the "Active Shooter (AS)" reference threat.*

Crosslink to J100 Standard Reference Threats	Annual Default Threat Likelihood Range Low: 10^{-6} to 10^{-5}
Aircraft: (A1) Helicopter, (A2) Small plane, (A3) Regional jet, (A4) Large jet **Assault Team:** (AT1) 1 Assailant, (AT2) 2-4 Assailants, (AT3) 5-8 Assailants, (AT4) 9-16 Assailants **Maritime:** (M1) Small boat, (M2) Fast boat, (M3) Barge, (M4) Deep draft ship **Vehicle Borne Bomb:** (V1) Car, (V2) Van, (V3) Midsize truck, (V4) Large truck (18-wheeler)	**Basis for default threat likelihood range:** • An armed assault on a U.S. water system has never been reported.* • Currently available intelligence (public) provides no basis to elevate the threat likelihood nationally. • **Conservative estimate of threat likelihood:** Approximately one attack under this threat category among all public water systems nationally every 1 to 10 years. • **Elevate the threat likelihood** if warranted by information from local law enforcement or intelligence agencies.

**Does not include active shooter incidents, which are covered under the "Directed/Sabotage" threat category.*

Table 7b: Threat Deterrence Factors for Assault on Utility – Physical

Factor	Impact on Threat Deterrence	Analyst Notes
1. Do both central and remote water system facilities display strong visible physical security features (see Table 6, factor 2)?	• The presence of visible physical security features may deter an assailant by decreasing the assessed vulnerability.	

Table 7c: Resources for Assault on Utility – Physical

Resource	Web Link
ASCE 78-24 Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities (expected publication in June 2024)	https://www.asce.org/
AWWA G430-14 (R20) Security Practices for Operation and Management	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/87153630
CISA Personal Security Considerations Action Guide: Critical Infrastructure Workers	https://www.cisa.gov/resources-tools/resources/personal-security-considerations-action-guide
DHS Cybersecurity and Infrastructure Security Agency	https://www.cisa.gov/topics/physical-security
Domestic Security Alliance Council	https://www.dsac.gov/
EPA Resources to Design and Implement Physical Security Monitoring for Surveillance and Response Systems	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-physical-security-monitoring-surveillance
InfraGard	https://www.infragard.org/
Local Law Enforcement Agencies	N/A
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers
Water Information Sharing and Analysis Center	https://www.waterisac.org/

Table 8a: Threat Category: Intentional Contamination of Finished Water

Threat Category Definition: *An incident where a contaminant is deliberately introduced into the finished water storage or distribution system with the intent of poisoning consumers and/or contaminating infrastructure.*

Crosslink to J100 Standard Reference Threats	Annual Default Threat Likelihood Range Low: 10^{-6} to 10^{-5}
Contamination of product C(B) Biotoxin C(C) Chemical C(S) Explosive C(P) Pathogen C(R) Radionuclide	**Basis for default threat likelihood range:** • Minor incidents of distribution system tampering are reported infrequently.* • Available public intelligence has shown awareness and intent by terror groups to carry out this type of attack, but currently available intelligence provides no basis to elevate the threat likelihood nationally. • **Conservative estimate of threat likelihood:** Approximately one attack under this threat category among all public water systems nationally every 1 to 10 years. • **Elevate the threat likelihood** if warranted by information from local law enforcement or intelligence agencies.

*No reported incidents of intentional distribution system contamination are known to have impacted customers.

Table 8b: Threat Deterrence Factors for Intentional Contamination of Finished Water

Factor	Impact on Threat Deterrence	Analyst Notes
1. Does the distribution system infrastructure display strong visible security features to deter unauthorized access (e.g., security fencing and lighting, locked hatches, locking hydrants, video surveillance of distribution system facilities)?	• Strong physical access control and intrusion detection devices that are visible and secure from tampering may deter an assailant by decreasing the assessed vulnerability.	
2. Does the water system have a public backflow prevention program, stipulating the use and regular inspection of backflow prevention devices?	• Public awareness that backflow prevention is present may deter a potential assailant from exploiting distribution system contamination through backflow by decreasing the assessed vulnerability.	

Table 8c: Resources for Intentional Contamination of Finished Water

Resource	Web Link
ASCE 78-24 Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities (expected publication in June 2024)	https://www.asce.org/
AWWA G430-14(R20) Security Practices for Operation and Management	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/87153630
Domestic Security Alliance Council	https://www.dsac.gov/
InfraGard	https://www.infragard.org/
Local Law Enforcement Agencies	N/A
State and Major Urban Area Fusion Centers	https://www.dhs.gov/fusion-centers
Water Information Sharing and Analysis Center	https://www.waterisac.org/
AWWA M-14 Backflow Prevention and Cross Connection Control: Recommended Practices	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/207854849
AWWA G200-15 Distribution Systems Operation and Management	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/49068206
EPA Cross Connection Control Manual	https://www.epa.gov/sites/default/files/2015-09/documents/epa816r03002_0.pdf
EPA Decontamination for Drinking Water and Wastewater Utilities	https://www.epa.gov/waterutilityresponse/decontamination-drinking-water-and-wastewater-utilities
EPA Drinking Water and Wastewater Laboratory Network	https://www.epa.gov/waterlabnetwork
EPA Online Water Quality Monitoring Resources	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources
EPA Resources to Design and Implement Physical Security Monitoring for Surveillance and Response Systems	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-physical-security-monitoring-surveillance
EPA Water Contamination Response Resources	https://www.epa.gov/waterqualitysurveillance/water-contamination-response-resources

Resource	Web Link
Intentional Contamination of Water Distribution Networks: Developing Indicators for Sensitivity and Vulnerability	https://link.springer.com/article/10.1007/s00477-017-1415-y
National Academy of Sciences Drinking Water Distribution Systems: Assessing and Reducing Risks	https://www.nap.edu/catalog/11728/drinking-water-distribution-systems-assessing-and-reducing-risks

Table 9a: Threat Category: Intentional Contamination of Source Water

Threat Category Definition: *The deliberate contamination of a drinking water source with the intent of the contaminated water entering water system infrastructure. Applies to surface and groundwater sources. The contamination may occur outside the control of the water system. Does not apply to the improper storage or disposal of materials where contamination of water is unintended.*

Crosslink to J100 Standard Reference Threats	Annual Default Threat Likelihood Range Low: 10^{-6} to 10^{-5}
Intentional contamination of source water is not a J100 Standard reference threat. EPA has included it as a threat category here based on prior recognition as a potential target of attack[10] and distinct threat characteristics (e.g., ease of access). The contaminant types listed as reference threats for *Intentional Contamination of Finished Water* also apply to this threat category.	**Basis for default threat likelihood range:** • Contamination of drinking water sources has occurred regularly due to accidental or improper waste storage or disposal. These incidents have impacted consumers and infrastructure but are not regarded as malevolent attacks on a water system.* • Available public intelligence has shown awareness and intent by terror groups to carry out this type of attack, but currently available intelligence provides no basis to elevate the threat likelihood nationally. • **Conservative estimate of threat likelihood:** Approximately one attack under this threat category among all public water systems nationally every 1 to 10 years. • **Elevate the threat likelihood** if warranted by information from local law enforcement or intelligence agencies.

**Reported incidents of improper (typically illegal) waste disposal into drinking water sources are not known to have been carried out for the purpose of contaminating a water system.*

[10] https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf

Table 9b: Threat Deterrence Factors for Intentional Contamination of Source Water

Factor	Impact on Threat Deterrence	Analyst Notes
1. Do source water reservoirs and intakes display strong visible security features to deter unauthorized access (see Table 6, factor 2)? 2. Are visible intrusion detection devices (e.g., contact alarms, video monitoring) installed and secured to avoid tampering at source water reservoirs and intakes?	• Strong physical access control and intrusion detection devices that are visible and secure from tampering may deter an assailant by decreasing the assessed vulnerability.	
3. Are chemicals or waste products stored or readily accessible in the vicinity of a source water intake or wellfield, which could allow for an uncontrolled release that would contaminate the source water?	• A proximate source of contaminants may increase threat likelihood due lower risk of interdiction prior to attack. Alternatively, this factor may be treated as a proximity hazard under the J100 Standard.	
4. Is the water system's source water reservoir or intake (as applicable) easily accessible by boat or land?	• Easy access to a water reservoir or intake may increase threat likelihood due to higher assessed vulnerability and lower risk of interdiction prior to attack.	

Table 9c: Resources for Intentional Contamination of Source Water

Resource	Web Link
ASCE 78-24 Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities (expected publication in June 2024)	https://www.asce.org/
AWWA G430-14(R20) Security Practices for Operation and Management	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/87153630

Resource	Web Link
AWWA Water Science: Comparative Evaluation of Risk Management Frameworks for U.S. Source Waters	https://awwa.onlinelibrary.wiley.com/doi/full/10.1002/aws2.1125
Domestic Security Alliance Council	https://www.dsac.gov/
EPA Drinking Water and Wastewater Laboratory Network	https://www.epa.gov/waterlabnetwork
EPA Online Water Quality Monitoring Resources	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources
EPA Resources to Design and Implement Physical Security Monitoring for Surveillance and Response Systems	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-physical-security-monitoring-surveillance
EPA Water Contamination Response Resources	https://www.epa.gov/waterqualitysurveillance/water-contamination-response-resources
InfraGard	https://www.infragard.org/
Local Law Enforcement Agencies	N/A
Operational Guide to AWWA Standard G300 Source Water Protection, Second Edition	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/64049372
State and Major Urban Area Fusion Centers	https://www.dhs.gov/fusion-centers
Water Information Sharing and Analysis Center	https://www.waterisac.org/

Table 10a: Threat Category: Theft or Diversion – Physical

Threat Category Definition: *A major incident of physical theft or diversion of critical resources, equipment, supplies, or infrastructure materials with the potential to disrupt the operations of a water system.*

Crosslink to J100 Standard Reference Threats	Annual Default Threat Likelihood Range Medium: 0.01 – 0.1*
Theft or Diversion T(PI) Physical-insider T(PU) Physical-outsider	**Basis for default threat likelihood range:** • Theft/diversion is commonplace at water systems, but most incidents do not have the potential to interfere with operations. • Water system theft incidents are not reported or tracked nationally. Default threat likelihood values reflect anecdotal information. • Individual water system theft history can provide the best basis for estimating this threat. • **Conservative estimate of threat likelihood:** Individual water systems have a likelihood of 1 to 10 percent annually of experiencing theft/diversion with the potential to interfere with operations. • **Elevate the threat likelihood** if warranted based on water system history or information from local law enforcement or intelligence agencies.

** This threat likelihood range applies only to a major incident of physical theft or diversion with the potential to disrupt the operations of a water system. It matches the range assigned to Directed/Sabotage – physical because both categories involve physical acts against water system infrastructure or resources that may disrupt operations.*

Table 10b: Threat Deterrence Factors for Theft or Diversion – Physical

Factor	Impact on Threat Deterrence	Analyst Notes
1. Does the water system physically secure high-value equipment, supplies and materials (e.g., secure fencing, lighting)? 2. Are intrusion detection devices (e.g., video monitoring) installed and secured at storage facilities?	• Strong visible physical security and intrusion detection devices that are secure from tampering may deter an assailant by decreasing the assessed vulnerability.	

Factor	Impact on Threat Deterrence	Analyst Notes
3. Are contractors and suppliers vetted for security purposes prior to gaining site access?	• Rigorous background checks of third parties (e.g., contractors, vendors, IT service providers) prior to authorizing access may deter an assailant by increasing risk of interdiction prior to initiation.	
4. Does the water system have the capability for rapid detection of theft or diversion, such as maintaining an updated inventory of materials and supplies? 5. Does the water system have an established process to ensure that thefts are investigated and that security gaps are eliminated?	• Rapid detection of theft or diversion followed by investigation and mitigation of security gaps may deter an assailant by decreasing the assessed vulnerability.	

Table 10c: Resources for Theft or Diversion – Physical

Resource	Web Link
ASCE 78-24 Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities (expected publication in June 2024)	https://www.asce.org/
AWWA G430-14(R20) Security Practices for Operation and Management	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/87153630
DHS Cybersecurity and Infrastructure Security Agency	https://www.cisa.gov/topics/physical-security
Domestic Security Alliance Council	https://www.dsac.gov/
EPA Resources to Design and Implement Physical Security Monitoring for Surveillance and Response Systems	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-physical-security-monitoring-surveillance
InfraGard	https://www.infragard.org/

Resource	Web Link
Local Law Enforcement Agencies	N/A
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers
Water Information Sharing and Analysis Center	https://www.waterisac.org/

Table 11a: Threat Category: Directed/Sabotage – Physical

Threat Category Definition: *Causing harm by damaging, disabling, or destroying equipment or infrastructure. Also includes active shooter incidents.*

Crosslink to J100 Standard Reference Threats	Annual Default Threat Likelihood Range Medium: 0.01 – 0.1
Directed/Sabotage-Physical S(PI) Physical-insider S(PU) Physical-outsider AS Active shooter	**Basis for default threat likelihood range:** • Incidents of physical process sabotage, both insider and outsider, are rare at water systems in the United States. • Physical process sabotage in other critical infrastructure sectors has been reported recently. • Active shooter incidents impacting water systems have been reported. • **Conservative estimate of threat likelihood:** Individual water systems have a likelihood of 1 to 10 percent annually of being targeted for physical process sabotage. Estimating the probability of an active shooter incident is not possible, but the same default likelihood is assigned to this threat due to significant public concern and recent incidents. • **Elevate the threat likelihood** if warranted based on water system history or information from local law enforcement or intelligence agencies.

Table 11b: Threat Deterrence Factors for Directed/Sabotage – Physical

Factor	Impact on Threat Deterrence	Analyst Notes
1. Do both central and remote water system facilities display strong visible physical security features (see Table 6, factor 2)?	• The presence of visible physical security features may deter an assailant by decreasing the assessed vulnerability.	

Factor	Impact on Threat Deterrence	Analyst Notes
2. Are contractors and suppliers vetted for security purposes prior to gaining site access?	• Rigorous background checks of third parties (e.g., contractors, vendors, IT service providers) prior to authorizing access may deter an assailant by increasing risk of interdiction prior to initiation.	
3. Does the water system take a proactive approach to address infrastructure damage or vandalism (e.g., graffiti at unmanned locations) that could indicate vulnerabilities?	• Remediating acts of vandalism and mitigating associated vulnerabilities may deter an assailant by decreasing the assessed vulnerability.	

Table 11c: Resources for Directed/Sabotage – Physical

Resource	Web Link
ASCE 78-24 Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities (expected publication in June 2024)	https://www.asce.org/
AWWA G430-14(R20) Security Practices for Operation and Management	https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/87153630
CISA Personal Security Considerations Action Guide: Critical Infrastructure Workers	https://www.cisa.gov/resources-tools/resources/personal-security-considerations-action-guide
DHS Cybersecurity and Infrastructure Security Agency	https://www.cisa.gov/topics/physical-security
Domestic Security Alliance Council	https://www.dsac.gov/
EPA Resources to Design and Implement Physical Security Monitoring for Surveillance and Response Systems	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-physical-security-monitoring-surveillance
InfraGard	https://www.infragard.org/
Local Law Enforcement Agencies	N/A

Resource	Web Link
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers
Water Information Sharing and Analysis Center	https://www.waterisac.org/

Table 12a: Threat Category: Cyberattack

Threat Category Definition: The J100 Standard includes the following definition of a cyberattack:

> *A type of man-made attack against the financial infrastructure (e.g., business/enterprise systems), which may include finance and budgeting, accounting, payroll, billing and receivables, personnel files, customer files, etc.), and process control systems or other automated systems that support utility operations (e.g., supervisory control and data acquisition, advanced metering infrastructure, energy management systems). Cyber threats can have a direct physical impact on critical infrastructure.*

Crosslink to J100 Standard Reference Threats	Annual Default Threat Likelihood High: 1

Cyber
C(1) Cyberattack
	Basis for default threat likelihood:
	• Cyberattacks are the highest risk malevolent act carried out against water systems (and other critical infrastructure).
	  ○ Disabling cyberattacks affecting business enterprise are reported frequently. Targeting of operational technology/process control systems is growing in frequency.
	  ○ Monitoring for active and passive attempted cyberattacks indicates a high incidence for accessible networks.
	• Law enforcement and intelligence agencies find that cyberattacks against water systems and other critical infrastructure are increasing.
	  ○ Artificial intelligence, increased automation, and other factors are expanding the vulnerability of water systems to cyberattacks.
	• The J100 Standard recommends this value.
	• **Conservative estimate of threat likelihood:** All water systems on average will experience at least one attempted cyberattack annually.

For all water system risk assessments, EPA recommends using an annual threat likelihood value of 1 for cyberattacks, consistent with the J100 Standard. Due to the high and growing frequency of attempted cyberattacks targeting critical infrastructure networks, EPA has not identified deterrence factors that support a lower threat likelihood value. Instead, EPA recommends that water systems utilize the resources listed in Table 12b, as well as other public and private sector resources available to the water system, to identify and adopt cybersecurity best practices that can reduce their vulnerability to and consequences from a cyberattack. Reported cyberattacks against water systems often exploit the failure to adopt basic cybersecurity best practices.

Table 12b: Resources for Cyberattack

Resource	Web Link
AWWA Water Sector Cybersecurity Risk Management Guidance. and Assessment Tool	https://www.awwa.org/Resources-Tools/Resources/Cybersecurity-Guidance
CISA Cross-Sector Cybersecurity Performance Goals	https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
CISA, EPA, and FBI Water and Wastewater Sector Incident Response Guide	https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0
CISA National Critical Functions – Supply Water and Manage Wastewater	https://www.cisa.gov/national-critical-functions-supply-water-and-manage-wastewater
CISA Top Cyber Actions for Securing Water Systems	https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems
CISA Water and Wastewater Cybersecurity	https://www.cisa.gov/water
EPA Cybersecurity for the Water Sector	https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector
National Security Agency Cybersecurity Advisory – Stop Malicious Cyber Activity Against Connected Operational Technology	https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF
NIST Cybersecurity Framework	https://www.nist.gov/cyberframework
NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security	https://csrc.nist.gov/pubs/sp/800/82/r3/final
NIST National Cybersecurity Center of Excellence: Securing Water and Wastewater Utilities	https://www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities
Water Information Sharing and Analysis Center	https://www.waterisac.org/
WaterISAC Cybersecurity Fundamentals for Water and Wastewater Utilities	http://www.waterisac.org/fundamentals

References

American Water Works Association. 2021. Risk and Resilience Management of Water and Wastewater Systems, J100-21. Available at: https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/88116441.

America's Water Infrastructure Act of 2018, Pub. L. No. 115-270, S. 3021, 115th Cong. Available at: https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf.

Brashear, Jerry, and Jones, James. 2010. Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus). *Wiley Handbook of Science and Technology for Homeland Security*. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470087923.hhs003.

U.S. Department of Homeland Security (DHS). 2013. National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience. Retrieved from: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.