United States
Environmental Protection
Agency

Baseline Information on Malevolent Acts for Community Water Systems

Office of Water (MC 140) EPA 817-K-19-001 November 2019

Disclaimer

The Water Security 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 imply 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 concerning this document should be addressed to WQ_SRS@epa.gov or the following contact:

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

Table of Contents

Disclaimer i

Abbreviations iv

Introduction 1

Section 1: AWIA Requirements 2

Section 2: Assessing Risk and Resilience 3

Section 3: Asset Categories 5

Section 4: Threat Categories and Likelihoods for Malevolent Acts 7

4.1 Threat Categories 7

4.2 Threat Likelihood 8

4.2.1 Factors for Estimating Threat Likelihood That Apply to Multiple Threat Categories 8

4.2.2 Factors for Estimating Threat Likelihood Values that Apply to Specific Threat Categories 10

Section 5: Resources for Additional Information 41

References 46

List of Figures

Figure 1: Critical Infrastructure Risk Management Framework....3

List of Tables

Table 1: AWIA Requirements and Certification Deadlines by CWS Size....2
Table 2: Approach to Risk Management....4
Table 3: AWIA-Identified Assets....5
Table 4: EPA Threat Categories for Malevolent Acts....7
Table 5: Factors for Threat Likelihood....8
Table 6: Threat Category: Assault on Utility – Physical....11
Table 7: Threat Category: Contamination of Finished Water – Accidental....14
Table 8: Threat Category: Contamination of Finished Water – Intentional....17
Table 9: Threat Category: Theft or Diversion – Physical....20
Table 10: Cyber Attack (Business Enterprise Systems and Process Control Systems)....23
Table 11: Threat Category: Sabotage – Physical....28
Table 12: Threat Category: Contamination of Source Water – Accidental....31
Table 14: Threat Category Resource Descriptions....41

Abbreviations

AWIA	America's Water Infrastructure Act of 2018
AWWA	American Water Works Association
CWS	Community Water System
DHS	U.S. Department of Homeland Security
EPA	U.S. Environmental Protection Agency
EPCRA	Emergency Planning and Community Right-to-Know Act
ERP	Emergency Response Plan
FBI	Federal Bureau of Investigation
IT	Information Technology
LEPC	Local Emergency Planning Committee
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
RAMCAP	Risk Analysis and Management for Critical Asset Protection
SDWA	Safe Drinking Water Act
SERC	State Emergency Response Commission
SLTT	State, Local, Tribal, Territorial
VSAT	Vulnerability Self-Assessment Tool
WaterISAC	Water Information Sharing & Analysis Center

Introduction

Dependable and safe water infrastructure is essential to human health and the nation's economy. Water systems, like other utilities, can face an array of threats from both natural hazards (e.g., floods, hurricanes) and malevolent acts (e.g., cyber-attacks, contamination). By using this document, systems can identify malevolent acts and take steps to reduce the risk that a specific system will experience if one occurs or potentially deter a threat from occurring.

By assessing threats, systems across the country can identify, prepare for and manage any risks they may have by adopting an "all-hazards" approach that:

- Identifies, deters, detects, and prepares for these threats.
- Reduces vulnerabilities of critical assets.
- Mitigates the potential consequences of incidents that do occur.

Pursuant to the requirements of America's Water Infrastructure Act (AWIA) Section 2013(a), the U.S. Environmental Protection Agency (EPA), in consultation with federal, state, and local government partners, has developed this guidance document to provide baseline information regarding malevolent acts of relevance to Community Water Systems (CWSs).[1]

The information included in this document is not a threat analysis for a specific system and it should not be used as such. The values are intended to serve as a starting point for systems to consider when they are estimating the threat likelihood of malevolent acts as part of a risk and resilience assessment.[2] When conducting site-specific assessments, systems may determine that lower or higher threat likelihood values are appropriate. The process systems will go through to identify their specific threats will account for their unique situations, which cannot be reflected in the baseline numbers. It is also important to note that threat likelihood is not an assessment of the risk that malevolent acts may have on public health.

While the resources provided in this document are already publicly available, this is the first time EPA, or any other federal agency, has compiled this important information for systems across the country. The 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 Likelihoods for Malevolent Acts** – Describes threat categories of relevance to CWSs.
- **Section 5: Resources for Additional Information** – Contains a listing of other sources of information on malevolent acts relevant to CWSs.

Water systems exhibit significant variability in assets, operations, system design, and other characteristics that influence the risk presented by different malevolent acts. Consequently, some information in this document may not be relevant to certain systems.

---

[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

Enacted as Public Law No: 115-270 on October 23, 2018, America's Water Infrastructure Act (AWIA) (https://www.congress.gov/bill/115th-congress/senate-bill/3021/text) establishes new risk and resiliency requirements for CWSs. Section 2013 of AWIA amends Section 1433 of the Safe Drinking Water Act (from the 2002 Public Health Security and Bioterrorism Response Act) and requires all CWSs serving more than 3,300 people to conduct Risk and Resilience Assessments that consider the risk to the system from malevolent acts and natural hazards (i.e., an "all-hazards" approach). The law also requires CWSs to update Emergency Response Plans (ERPs). AWIA specifies the components that the Risk and Resilience Assessments and ERPs must address and establishes the deadlines in **Table 1** to certify completion to EPA.

Safeguarding Sensitive Information

Risk and Resilience Assessments and Emergency Response Plans contain sensitive information that should be protected from inadvertent disclosure. Utilities should establish procedures to control sensitive information as they develop and update these documents.

Table 1: AWIA Requirements and Certification Deadlines by CWS Size

Population Served	Certification Deadlines	
	Risk Assessment	Emergency Response Plan*
≥100,000	March 31, 2020	September 30, 2020
50,000-99,999	December 21, 2020	June 30, 2021
3,301-49,999	June 30, 2021	December 30, 2021

*ERP certifications are due as soon as possible and no later than 6 months from the date of the risk assessment certification to EPA. The ERP dates shown are certification dates based on a utility submitting a risk assessment on the final due date.

To assist utilities in identifying threats to be considered in Risk and Resilience Assessments, AWIA Section 2013 directs 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.

5-Year Review and Revision

AWIA requires each CWS serving more than 3,300 people to:

- Review its Risk and Resilience Assessment at least every 5 years to determine if it should be revised.
- Submit to EPA a certification that it has reviewed and, if necessary, revised its assessment.
- Revise, as necessary, its ERP at least every 5 years after completing the Risk and Resilience Assessment review.
- Submit to EPA a certification that it has reviewed and, if necessary, revised its ERP within 6 months after certifying the review of its Risk and Resilience Assessment.

This document provides baseline threat information related to malevolent acts, as required by AWIA, as well as an overview of how this information may be used in the risk assessment process. Natural hazards are not included in the scope of this document.

Section 2: Assessing Risk and Resilience

Under the 2013 *National Infrastructure Protection Plan* (NIPP), *Critical Infrastructure Risk Management Framework*,[3] critical infrastructure risks can be assessed in terms of the following:

- **Threat** – natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability** – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- **Consequence** – effect of an event, incident, or occurrence.

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood (a function of threats and vulnerabilities) and the associated consequences. Threat likelihood in this document does not refer to public health impacts, but rather the likelihood of a threat happening to a CWS. Risk assessments identify the most significant malevolent acts and natural hazards to a CWS's critical assets, systems, and networks. A risk assessment for a CWS accounts for threats to source water (ground and surface), treatment and distribution systems, and business enterprise systems. It also considers risks posed to the surrounding community related to attacks on the CWS. An effective risk assessment serves as a guide to facilitate a prioritized plan for security upgrades, modifications of operational procedures, and policy changes to mitigate the risks to the CWS's critical assets.

This document is not a risk assessment tool. Instead, it presents an overview of the baseline threat posed by malevolent acts, which can be reviewed prior to and when conducting a Risk and Resilience Assessment. ("Baseline" in this context is an ongoing level, which may be elevated situationally.) CWSs may select any appropriate risk assessment standard, methodology, or tool that assists in meeting the requirements of AWIA Section 2013. Regardless of the use of any standard, methodology or tool, the CWS is responsible for ensuring that its Risk and Resilience Assessment and ERP fully address all applicable AWIA requirements.

As described in the 2013 NIPP, a Risk and Resilience Assessment is one component of an overall Risk Management Framework, as shown in **Figure 1** (from Figure 3 of the 2013 NIPP). The nature and extent of the risk assessment will differ among systems based on a range of factors, including system size, potential population affected, source water, treatment complexity, system infrastructure, and other factors. Regardless of these considerations, 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, systems can use the results of the risk assessment to maximize short- and long-term risk reduction and resilience within available resources.

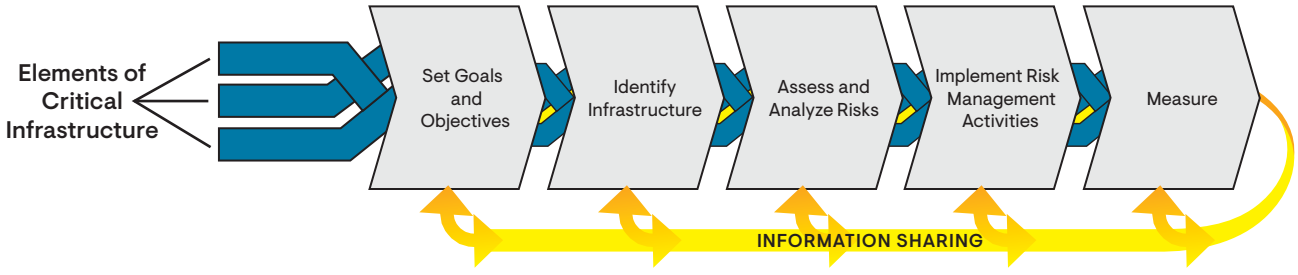

Figure 1: Critical Infrastructure Risk Management Framework

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

Table 2: Approach to Risk 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

Under AWIA Section 2013, each CWS serving more than 3,300 people is required to assess the risk to the system from malevolent acts and natural hazards for the asset categories listed in **Table 3.**[4] Note that the asset categories in **Table 3** are taken directly from AWIA Section 2013(a).[5] The EPA examples for each of the asset categories are offered as guidance only and will not apply to all systems. Each CWS must identify the critical assets to be assessed under AWIA based on system type and design.

Table 3: AWIA-Identified Assets

Asset Categories	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.[6]
Source water	Encompasses all sources that supply water to a CWS. Possible examples include rivers, streams, lakes, source water reservoirs, groundwater, and purchased water.
Pipes and constructed conveyances, water collection, and intake	Encompasses the infrastructure that collects and transports water from a source water to treatment or distribution facilities. Possible examples include holding facilities, intake structures and associated pumps and pipes, aqueducts, and other conveyances.
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 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).

[4] 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.

[5] See the AWIA's amended language for Section 1433(a)(1)(A) of the Safe Drinking Water Act.

[6] 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 degraded.

Asset Categories	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. Examples are contamination warning systems for the source water or distribution system.[7]
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 on the risk of uncontrolled release of a potentially dangerous chemical like chlorine where applicable.
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. Possible examples include equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like loss of utilities (e.g., power outage), loss of suppliers (e.g., interruption in chemical delivery), and loss of key employees (e.g., disease outbreak or employee displacement).

[7] 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 Likelihoods for Malevolent Acts

This section provides baseline information on malevolent acts of relevance to CWSs.[1]

4.1 Threat Categories

As guidance for AWIA compliance, EPA has identified **threat categories** for malevolent acts, as 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 subject to the requirements of AWIA Section 2013 consider this information when conducting the Risk and Resilience Assessment.

Table 4: EPA Threat Categories for Malevolent Acts

EPA Threat Categories
Assault on Utility – Physical
Contamination of Finished Water – Accidental*
Contamination of Finished Water – Intentional
Theft or Diversion – Physical
Cyber Attack on Business Enterprise Systems
Cyber Attack on Process Control Systems
Sabotage – Physical
Contamination of Source Water – Accidental*
Contamination of Source Water – Intentional

*Accidental contamination threat categories are not malevolent acts but are included here due to similar potential consequences. Further, whether a contamination incident is intentional or accidental may not be known during initial response. These threat categories are also grouped with malevolent acts in EPA's Vulnerability Self-Assessment Tool (VSAT) Web Version 2.0.

EPA considered the larger body of Reference Threats from AWWA J100-10 *Risk and Resilience Management of Water and Wastewater Systems* when creating these broad Threat Categories (Table 4).[8] The J100-10 Reference Threats were adapted for water systems from *Risk Analysis and Management for Critical Asset Protection,* which was developed by the American Society of Mechanical Engineers and endorsed by the Department of Homeland Security for critical infrastructure protection.[9]

EPA grouped the AWWA J100-10 Reference Threats into a smaller number of threat categories in order to simplify the Risk and Resilience Assessment process. Note that the threat categories are incorporated into VSAT Web Version 2.0, which can be used to comply with the AWIA Risk and Resilience Assessment requirements for CWSs.[10] Malevolent acts may be perpetrated by individuals or groups operating outside or inside the CWS.

[8] American Water Works Association, *J100-10 (R13) Risk and Resilience Management of Water and Wastewater Systems* (Washington, DC, 2013)

[9] 2006 National Infrastructure Protection Plan, U.S. Department of Homeland Security https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf

[10] https://vsat.epa.gov/vsat/

4.2 Threat Likelihood

Threat likelihood can be impacted by many factors, such as adversary intent and capability; target visibility and potential impact; awareness, ease of discovery, and ease of exploitation of CWS vulnerabilities; and the probability of detection and intervention. Deriving an accurate quantitative estimate of threat likelihood for malevolent acts based on underlying risk factors is challenging and may be outside the capability of a CWS. Such an estimate may require information that is not available to the CWS, even with the engagement of law enforcement and intelligence agencies.

To assist CWSs with conducting Risk and Resilience Assessments under AWIA, EPA has provided default threat likelihood values for each of the threat categories. These default values are general, order-of-magnitude estimates that are intended to serve as a starting point for the Risk and Resilience Assessment. 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.

Characteristics of the facility or system being assessed, along with information from local law enforcement, intelligence agencies, and other credible sources as described below, can support the development of site-specific threat likelihood values. Further, systems may choose to estimate threat likelihood using alternate methods, such as the Proxy Method described in the AWWA J100-10 Standard.

4.2.1 Factors for Estimating Threat Likelihood That Apply to Multiple Threat Categories

Prior to showing the individual threat category tables, **Table 5** presents factors for threat likelihood that apply to multiple threat categories. EPA recommends reviewing this list when assessing the likelihood that a malevolent actor would target your system or facility. These factors can be indicators of the general threat environment for a system or facility. They should be evaluated in combination with the factors for specific threat categories, as discussed in the next section, when making a site-specific threat likelihood estimate.

Table 5: Factors for Threat Likelihood

Factor	Considerations	Notes
1. Does the utility serve a major population center or prominent facility?	· Utilities that serve large population centers or prominent facilities (e.g., large government installation) may have a greater likelihood of high consequence threats (e.g., intentional contamination, cyber process control attack, physical assault) by a sophisticated attacker due to increased public health and economic impacts and high visibility. · Smaller and medium utilities may have a higher likelihood of an unsophisticated threat (e.g., cyber business enterprise attack, sabotage) due to fewer security resources.	
2. How difficult are the logistics of an attack on the utility infrastructure, and what measures are in place to deter an attack?	· Ease of access (physical or electronic) to facilities, systems, and infrastructure can increase threat likelihood. · The presence of visible physical and electronic security can deter an attacker (reduced threat likelihood).	

Factor	Considerations	Notes
3. Are there critical points in the utility infrastructure or operations where an attack could achieve complete disruption of the utility's capability to supply safe drinking water?	· A single point of failure (e.g., single source of water, single water storage tank) for utility operations may increase the likelihood of an attack at that point. · Redundant systems that increase resilience may reduce threat likelihood.	
4. Does the utility have protocols for responding to disgruntled or hostile employees and customers?	· A utility culture that fails to resolve workplace complaints can increase the likelihood of an insider threat (e.g., sabotage, theft). · Similarly, unaddressed issues with upset customers could increase the likelihood of a physical attack, theft, or vandalism.	
5. Are non-employees with access to systems or facilities properly vetted?	· Rigorous background checks of third parties with access to utility facilities or systems (e.g., contractors, vendors, IT service providers) prior to authorizing access, can reduce threat likelihood of a third-party insider attack.	
6. Do organizations with extremist political, social, or other ideologies operate in the vicinity of my utility?	· Proximity to extremist organizations may increase the likelihood of external physical threats, such as intentional contamination, sabotage, or assaults. Intelligence and law enforcement information on the capabilities and intent of an organization should be evaluated.	
7. Has the facility been the target of previous physical or cyberattacks?	· Previous attacks may increase the threat likelihood of similar attacks in the future if they reveal security weaknesses or inspire copycat attacks.	
8. Are senior managers at the utility, as well as other responsible personnel (e.g., water board, local government) actively engaged in threat assessments and risk management?	· Commitment to establishing a culture of security by the utility and local government (e.g., resources, integration of security best practices) can achieve a broad reduction in the likelihood of malevolent acts.	

4.2.2 Factors for Estimating Threat Likelihood Values that Apply to Specific Threat Categories

Tables 6 – 13 (threat categories) presented below include:

- Corresponding reference threats from the AWWA J100-10 Standard
- Basis for EPA default threat likelihood values
- Factors for estimating site-specific threat likelihood values
  - The factors are presented as yes/no questions for a CWS. As described further below, the responses of a CWS to these questions may indicate whether a site-specific threat likelihood estimate for the CWS would be higher or lower than the EPA default value.
- Publicly available resources for additional information

While AWIA Section 2013 is applicable only to drinking water systems, default threat likelihoods for wastewater systems, which are included in VSAT Web 2.0, are also shown in the tables.

Completion of Threat Category Checklists and Interpretation of Results

1. The checklist questions in Tables 6 - 13 below are intended to help CWSs assess how their current capabilities and operating environment may either deter a malevolent actor and decrease threat likelihood or suggest a higher likelihood of attack.
2. Select “yes” or “no” for each question. A worksheet is provided after each checklist to allow CWSs to capture notes relevant to their current capabilities and operations for future reference when completing the Risk and Resilience Assessment and Emergency Response Plan.
3. If mostly “yes” answers are selected for an individual threat category, then a lower site-specific threat likelihood estimate may be warranted. Conversely, if mostly “no” answers are selected, then a higher site-specific threat likelihood may be appropriate. A mix of “yes” and “no” responses would support the applicability of the default threat likelihood value. CWSs should consult the resources listed for each threat category when evaluating modifications to threat likelihood values.
4. Further, “no” responses may inform actionable steps a CWS might consider for reducing risk by implementing additional countermeasures.

Table 6: Threat Category: Assault on Utility – Physical

Threat Category Definition: *A physical assault on utility infrastructure or staff with the intent of disabling infrastructure and/or terrorizing staff*

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
• **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 • **Directed:** (AS) Active Shooter • **Contamination of Product:** C(E) Explosive	10^{-6}	10^{-6}
	Basis: • Estimate 100,000 potential water utility targets in the United States. • While this type of attack is possible, it has never been reported for a U.S. water utility. • Available intelligence (public) provides no basis to elevate this likelihood currently. • **Conservative estimate of threat likelihood:** One attack per 10 years among 100,000 water utilities.	

Factors for Modifying Default Threat Likelihood

1. Has strict access control been implemented at utility facilities (e.g., visitor restrictions and logging, electronic employee access systems with logging, locked windows, grates, doors, and other access points, intrusion alarms, video monitoring with recording, security personnel)?
   ◯ Yes ◯ No
2. Are physical barriers in place at treatment facilities to impede unauthorized access (include waterway access if applicable)?
   ◯ Yes ◯ No
3. Are physical barriers in place in place at isolated assets such as storage tanks, well fields, and intakes to impede unauthorized access?
   ◯ Yes ◯ No
4. Are intrusion detection devices (e.g., contact alarms, video monitoring) installed and monitored at distribution system facilities?
   ◯ Yes ◯ No
5. Are procedures in place for rapid response and investigation of alarms or other indicators of unauthorized entry?
   ◯ Yes ◯ No
6. Are intrusion detection devices properly maintained to avoid frequent false alarms resulting in “alarm fatigue”?
   ◯ Yes ◯ No
7. Are alarm and electronic surveillance systems secure to avoid tampering?
   ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
ASCE, Guidelines for the Physical Security of Water Utilities (56-10) *and Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (57-10)	https://ascelibrary.org/doi/book/10.1061/9780784411261	1
AWWA G430-14 *Security Practices for Operation and Management*	https://www.awwa.org/Store/Product-Details/productId/45320372	2
Domestic Security Alliance Council	https://www.dsac.gov/	3
InfraGard	https://www.infragard.org/	4
Local Law Enforcement Agencies	N/A	5
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers	6
Water Information Sharing and Analysis Center	https://www.waterisac.org/	7

Notes

1.
2.
3.
4.
5.
6.
7.

Table 7: Threat Category: Contamination of Finished Water – Accidental[11]

Threat Category Definition: *An incident where contamination of finished water in the storage or distribution system occurs due to an unintentional operational, management, or design failure such as pressure loss, leaking infrastructure, or cross connection*

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Contamination of Product: C(C) Chemical, C(P) Pathogen	0.2	N/A
	Basis: • Accidental contamination of finished water occurs at U.S. water utilities. Most incidents are minor and do not have measurable public health or economic consequences. • Major incidents of accidental microbial or chemical contamination of finished water can occur with significant adverse impacts on the utility and surrounding community. • Potential causes of accidental contamination include cross-connections, backflow, breaches in the integrity of storage facilities, and infiltration during periods of low pressure. • **Conservative estimate of threat likelihood:** Utilities experience accidental contamination of finished water twice per year, and 10% of these incidents have significant public health or economic consequences.	

Factors for Modifying Default Threat Likelihood

1. Has the utility's distribution system management been effective in preventing accidental contamination events in the recent past (e.g., the past five years)?
   ◯ Yes ◯ No
2. Do operators receive regular training on procedures for distribution system monitoring and operations?
   ◯ Yes ◯ No
3. Are the personnel who conduct work in the distribution system (e.g., installing pipes, repairing broken water mains) properly trained to prevent contamination of drinking water infrastructure?
   ◯ Yes ◯ No
4. Are storage tanks routinely inspected for possible damage/aging?
   ◯ Yes ◯ No

[11] Accidental contamination of finished water is not a malevolent act but is included here due to similar potential consequences with intentional contamination. This threat category is also grouped with malevolent acts in EPA's *Vulnerability Self-Assessment Tool (VSAT) Web Version 2.0.*

5. Does the utility have a backflow prevention program, stipulating the use and regular inspection of backflow prevention devices?
   ◯ Yes ◯ No

6. Are online water quality monitoring devices (e.g., chlorine residual, pressure monitoring, advanced metering) used in the distribution system to provide early detection of system integrity or operational problems?
   ◯ Yes ◯ No

7. If hazardous contaminants are produced or stored in the vicinity of the distribution system, has the utility communicated with the responsible party regarding proper containment of those contaminants (to avoid contaminant intrusion during low pressure events)?
   ◯ Yes ◯ No

8. Has the utility performed a sanitary survey that includes distribution system components within the last 3 years?
   ◯ Yes ◯ No

9. Has the utility performed a condition assessment of its distribution system assets within the last 5 years?
   ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions

Resource	Web Link	# in Section 5
AWWA M-14 *Backflow Prevention and Cross Connection Control: Recommended Practices*	https://www.awwa.org/Store/Product-Details/productId/46494412	8
AWWA G200-15 *Distribution Systems Operation and Management*	https://www.awwa.org/Store/Product-Details/productId/49065093	9
EPA *Cross Connection Control Manual*	https://www.epa.gov/sites/production/files/2015-09/documents/epa816r03002_0.pdf	10
EPA *Online Water Quality Monitoring Resources*	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources	11
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	12

Notes

1.
2.
3.
4.
5.
6.
7.
8.
9.

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

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 AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Contamination of Product: C(B) Biotoxin, C(C) Chemical, C(P) Pathogen, C(R) Radionuclide	10^{-5}	N/A
	Basis: • Estimate 100,000 potential water utility targets in the United States. • A few incidents of intentional finished water contamination have been reported in the United States and foreign countries over several decades. • Pilot studies and computer simulations have shown that this mode of attack can inflict very high consequences. • Available intelligence (public) indicates awareness and intent by terror groups to carry out this type of attack. • **Conservative estimate of threat likelihood:** One attack per year among 100,000 water utilities.	

Factors for Modifying Default Threat Likelihood[12]

1. Are physical barriers in place in place at isolated assets such as storage tanks, well fields, and intakes to impede unauthorized access?
   ◯ Yes ◯ No
2. Are intrusion detection devices (e.g., contact alarms, video monitoring) installed and monitored at distribution system facilities?
   ◯ Yes ◯ No
3. Are procedures in place for rapid response and investigation of alarms or other indicators of unauthorized entry?
   ◯ Yes ◯ No
4. Are intrusion detection devices properly maintained to avoid frequent false alarms resulting in "alarm fatigue"?
   ◯ Yes ◯ No
5. Are alarm and electronic surveillance systems secure to avoid tampering?
   ◯ Yes ◯ No
6. Does the utility have a backflow prevention program, stipulating the use and regular inspection of backflow prevention devices?
   ◯ Yes ◯ No

[12] Questions 1 – 5 apply to distribution system facilities and are also included in the *Threat Category: Assault on Utility – Physical,* which addresses physical barriers, intrusion detection, and alarm response, maintenance, and security. Question 6 is also included in the *Threat Category: Contamination of Finished Water – Accidental.*

7. Does the utility have a program to secure exposed distribution system access points (e.g., locking hydrants)?
   ◯ Yes ◯ No

8. Are utility staff trained to observe for potential hazards at distribution system facilities and access points, such as unauthorized pumper trucks using hydrants or storage tanks, indicators of tampering, empty chemical containers or hardware from non-utility sources?
   ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
ASCE, Guidelines for the Physical Security of Water Utilities (56-10) *and Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (57-10)	https://ascelibrary.org/doi/book/10.1061/9780784411261	1
AWWA G430-14 *Security Practices for Operation and Management*	https://www.awwa.org/Store/Product-Details/productId/45320372	2
Domestic Security Alliance Council	https://www.dsac.gov/	3
InfraGard	https://www.infragard.org/	4
Local Law Enforcement Agencies	N/A	5
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers	6
Water Information Sharing and Analysis Center	https://www.waterisac.org/	7
AWWA M-14 *Backflow Prevention and Cross Connection Control: Recommended Practices*	https://www.awwa.org/Store/Product-Details/productId/46494412	8
AWWA G200-15 *Distribution Systems Operation and Management*	https://www.awwa.org/Store/Product-Details/productId/49065093	9
EPA *Cross Connection Control Manual*	https://www.epa.gov/sites/production/files/2015-09/documents/epa816r03002_0.pdf	10
EPA *Online Water Quality Monitoring Resources*	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources	11
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	12

Resources (continued)		
Resource	**Web Link**	**# in Section 5**
EPA Resources to Design and Implement Enhanced Security Monitoring for Surveillance and Response Systems	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-enhanced-security-monitoring-surveillance	13

Notes

1.
2.
3.
4.
5.
6.
7.
8.

Table 9: Threat Category: Theft or Diversion – Physical

Threat Category Definition: *Any incident of physical theft or diversion of utility resources, supplies, and infrastructure materials*

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Theft or Diversion: T(PI) Physical-Insider, T(PU) Physical-Outsider	0.2	0.2
	Basis: • Theft/diversion is commonplace at water utilities, but most incidents do not have significant economic consequences. • Water utility theft incidents are not tracked nationally. • **Conservative estimate of threat likelihood:** Water utilities experience theft/diversion twice per year, and 10% of these incidents have significant economic consequences for the utility. No public health likelihood is projected.	

Factors for Modifying Default Threat Likelihood

1. Does the utility have an established process to ensure that thefts are investigated (by law enforcement or the utility), any security gaps that facilitated the theft are identified, and any such gaps are mitigated to reduce risk?
   ◯ Yes ◯ No

2. Are high-value utility supplies and materials physically secured on the premises and actively monitored to prevent theft?
   ◯ Yes ◯ No

3. Are contractors and suppliers vetted for security purposes prior to gaining site access?
   ◯ Yes ◯ No

4. Does the utility have the capability for rapid detection of theft or diversion, such as maintaining an updated inventory of materials and supplies?
   ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
ASCE, *Guidelines for the Physical Security of Water Utilities* (56-10) *and Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (57-10)	https://ascelibrary.org/doi/book/10.1061/9780784411261	1
AWWA G430-14 Security Practices for Operation and Management	https://www.awwa.org/Store/Product-Details/productId/45320372	2
Domestic Security Alliance Council	https://www.dsac.gov/	3
InfraGard	https://www.infragard.org/	4
Local Law Enforcement Agencies	N/A	5
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers	6
Water Information Sharing and Analysis Center	https://www.waterisac.org/	7

Notes

1.
2.
3.
4.

Threat Category: Cyber Attack

For the purpose of AWIA Risk and Resilience Assessments, EPA has grouped cyber-attacks on water utilities into two categories. One is cyber-attack on business enterprise systems, which include computer-based communications, financial, data and record keeping, and other related systems. The second is cyber-attack on process control systems, which includes electronic monitoring and control systems used for water collection, treatment, storage, and distribution across the utility.

Cyber-attacks on these two areas of a water utility have different threat likelihoods and consequences. Cyber penetration into and disruption of business enterprise systems (e.g., ransomware, data theft) has been reported at many CWSs (either as a direct attack on the utility or secondarily from an attack on a municipal network). While the response and recovery costs from cyber-attacks on business enterprise systems can be high, these attacks typically do not disrupt water service.

In contrast, cyber-attacks on water process control systems are not common. Most reported incidents of cyber penetration into process control systems have occurred where control networks lacked adequate segregation from business enterprise networks. However, intentional cyber penetration into U.S. water utility process control systems by rogue state actors has been reported, and cyber-attacks have disrupted critical process operations in other sectors (e.g., energy, manufacturing). Consequently, these attacks have the potential to disrupt water service.

Notwithstanding differences in risk, the factors for modifying EPA's default threat likelihood values for each cyber threat category are the same. Consequently, this document provides one list of factors for both cyber threat categories. The table that follows shows the default threat likelihood (and associated basis) for a cyber-attack on a business enterprise system, followed by a cyber-attack on a process control system, and then the factors for a site-specific threat likelihood estimate for both.

Table 10: Cyber Attack (Business Enterprise Systems and Process Control Systems)

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Business Enterprise Systems Threat Category Definition: *A cyber-attack on utility billing, communications, data management or other information systems, which may disable affected systems and result in the loss of information resources, including personal, financial and other sensitive data, and other economic consequences for the utility*		
• **Theft or Diversion:** T(CI) Cyber-Insider, T(CU) Cyber-Outsider • **Cyber Insider:** C(I1) Insider, C(I2) Trusted Insider/Accidental • **Cyber Outsider:** C(O1) Cyber Outsider Attackers, C(O2) Criminal Group, C(O3) Terrorist, C(O4) Foreign Intelligence Service	0.3	0.3
	Basis: • Cyber-attacks on business enterprise systems occur frequently at water utilities (and elsewhere). Many successful cyber-attacks involving water utility business enterprise systems have been reported, often with significant economic consequences for the utility. • **Conservative estimate of threat likelihood:** Water utilities experience an attempted cyber-attack on a business enterprise system once per year, and 30% of these incidents have the potential for significant economic consequences.	
Process Control Systems Threat Category Definition: *A cyber-attack on utility process control systems, including monitoring, operations, and centralized control. The attack may disable or manipulate utility infrastructure, potentially resulting in loss of service, the contamination of finished water and damage to utility infrastructure*		
• **Cyber Insider:** C(I1) Insider, C(I2) Trusted Insider/Accidental • **Cyber Outsider:** C(O1) Cyber Outsider Attackers, C(O2) Criminal Group, C(O3) Terrorist, C(O4) Foreign Intelligence Service	0.1	0.1
	Basis: • No successful cyber-attacks on U.S. water utility process control systems have been proven, though possible attacks have been reported. • Pilot-scale studies have demonstrated cyber capability to manipulate water utility valves and chemical dosing. • Water utilities use communications and control systems that are common across critical infrastructure sectors, and these systems have been penetrated by cyber-attacks in other sectors. • Available intelligence (public) indicates long-term cyber presence in U.S. critical infrastructure control systems by foreign state actors. • **Conservative estimate of threat likelihood:** Water utilities experience an attempted cyber-attack on a process control system once per year, and 10% of these incidents may have significant public health or economic consequences.	

Factors for Modifying Default Threat Likelihood

Does the utility:

1. Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility?
   ◯ Yes ◯ No

2. Employ staff with primary responsibility for and allocate a dedicated budget to the security and resiliency of electronic networks?
   ◯ Yes ◯ No

3. Address the security of electronic networks in relevant contracts, and ensure that contract staff with access to utility electronic networks are vetted?
   ◯ Yes ◯ No

4. Segregate networks and apply firewalls?
   ◯ Yes ◯ No

5. Use secure remote access methods?
   ◯ Yes ◯ No

6. Establish roles to control access to different networks and log system users?
   ◯ Yes ◯ No

7. Require strong passwords and password management practices?
   ◯ Yes ◯ No

8. Stay aware of vulnerabilities and implement patches and updates when needed?
   ◯ Yes ◯ No

9. Enforce policies for the security of mobile devices?
   ◯ Yes ◯ No

10. Have an employee cybersecurity training program?
    ◯ Yes ◯ No

11. Involve utility executives in cybersecurity?
    ◯ Yes ◯ No

12. Monitor for network intrusions and have a plan in place to respond?
    ◯ Yes ◯ No

13. Readily investigate possible network intrusions?
    ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
AWWA *Process Control System Security Guidance for the Water Sector* and Use-Case Tool	https://www.awwa.org/Resources-Tools/Resources/Cybersecurity-Guidance	14
DHS National Cybersecurity and Communications Integration Center	https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center	15
NIST Cybersecurity Framework	https://www.nist.gov/cyberframework	16
NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final	17
NIST SP 800-82 Revision 2, Guide to Industrial Control Systems Security	https://www.csiac.org/reference-doc/nist-sp-800-82-revision-2-guide-to-industrial-control-systems-ics-security/	18
WaterISAC *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*	www.waterisac.org/fundamentals	19

Notes

1.
2.
3.
4.
5.
6.
7.

Notes

8.
9.
10.
11.
12.
13.

Table 11: Threat Category: Sabotage – Physical

Threat Category Definition: *A malicious physical act that is carried out with the intention of causing adverse impacts on a utility process*

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Directed/Sabotage: S(PI) Physical-Insider, S(PU) Physical-Outsider	0.05	0.05
	Basis: • Malicious process sabotage is rarely reported at U.S. water utilities. However, incidents could have significant economic and public health consequences. • **Conservative estimate of threat likelihood:** Water utilities experience process sabotage once every ten years, and 50% of these incidents have significant economic consequences for the utility.	

Factors for Modifying Default Threat Likelihood[13]

1. Has strict access control been implemented at utility facilities (e.g., visitor restrictions and logging, electronic employee access systems with logging, locked windows, grates, doors, and other access points, intrusion alarms, video monitoring with recording, security personnel)?
   ◯ Yes ◯ No
2. Are physical barriers in place at treatment facilities to impede unauthorized access (include waterway access if applicable)?
   ◯ Yes ◯ No
3. Are physical barriers in place in place at isolated assets such as storage tanks, well fields, and intakes to impede unauthorized access?
   ◯ Yes ◯ No
4. Are intrusion detection devices (e.g., contact alarms, video monitoring) installed and monitored at distribution system facilities?
   ◯ Yes ◯ No
5. Are procedures in place for rapid response and investigation of alarms or other indicators of unauthorized entry?
   ◯ Yes ◯ No
6. Are intrusion detection devices properly maintained to avoid frequent false alarms resulting in "alarm fatigue"?
   ◯ Yes ◯ No
7. Are alarm and electronic surveillance systems secure to avoid tampering?
   ◯ Yes ◯ No

[13] Questions 1 – 7 are also included in the *Threat Category: Assault on Utility – Physical.*

8. Are contractors with knowledge of water utility operations and process control systems vetted prior to gaining access to utility property and assets?

   ◯ Yes ◯ No

9. Do critical utility process assets that could be subject to sabotage have built-in redundancies, such that the failure of a single process asset would not disrupt water service?

   ◯ Yes ◯ No

10. Does the utility take a proactive approach to address infrastructure damage or vandalism (e.g., graffiti at unmanned locations) that could indicate vulnerabilities?

    ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
ASCE, *Guidelines for the Physical Security of Water Utilities* (56-10) *and Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (57-10)	https://ascelibrary.org/doi/book/10.1061/9780784411261	1
AWWA G430-14 *Security Practices for Operation and Management*	https://www.awwa.org/Store/Product-Details/productId/45320372	2
Domestic Security Alliance Council	https://www.dsac.gov/	3
InfraGard	https://www.infragard.org/	4
Local Law Enforcement Agencies	N/A	5
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers	6
Water Information Sharing and Analysis Center	https://www.waterisac.org/	7

Notes

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Table 12: Threat Category: Contamination of Source Water – Accidental[14]

Threat Category Definition: *An unintentional incident of contamination of a drinking water source that could result in contaminated water entering the utility. Applies to surface and groundwater sources (including purchased). The contamination may occur outside the control of the utility.*

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Accidental contamination of source water is not included in the J100-10 Standard.	0.05	N/A
	Basis: • Accidental contamination of drinking water sources occurs regularly through spills, untreated discharges, infrastructure failures, and other causes. The contamination event is usually outside the control of the utility. • Reported spill data (National Response Center, 2010 -2017) showed an average of 1,100 spills per year that impacted sources of drinking water. Occurrence varied widely based watershed characteristics. • Upstream contamination typically does not cause significant economic or public health impacts for drinking water utilities due to dilution, natural attenuation and upstream mitigation actions. Utilities may be able to close affected intakes. • If contaminated source water enters the treatment plant, it may damage infrastructure and affect public health. • **Conservative estimate of threat likelihood:** On average, 5% of water utilities experience a source water contamination event that impacts water quality.	

Factors for Modifying Default Threat Likelihood

Systems with a Surface Water Source

1. Has the utility avoided a source water contamination event in the recent past (e.g., the past 5 years) due to source water characteristics and management, intake operation, and other factors?
   ◯ Yes ◯ No

2. Does the utility have multiple intakes positioned in a manner that could mitigate the impacts of a spill (e.g., on different reaches of a water body or at different depths)?
   ◯ Yes ◯ No

3. Is the utility's watershed relatively pristine and free of significant sources of potential contamination (e.g., storage reservoirs and tanks, railways, hazmat routes, dischargers, agricultural areas, hazardous waste site)?
   ◯ Yes ◯ No

[14] Accidental contamination of source water is not a malevolent act but is included here due to similar potential consequences with intentional contamination. This threat category is also grouped with malevolent acts in EPA's *Vulnerability Self-Assessment Tool (VSAT) Web Version 2.0.*

4. Is the utility's source water free of watercraft and waterborne cargo?
   ◯ Yes ◯ No

5. Has the region impacting the utility's watershed taken steps to mitigate the risk of chronic water quality issues (e.g., nutrient loading) from turning into serious problems (e.g., harmful algal blooms)?
   ◯ Yes ◯ No

6. Has the utility coordinated with upstream authorities and facilities that are potential sources of contamination for timely notification in the event of a spill or release into the utility's source water?
   ◯ Yes ◯ No

7. Does the utility have a source water monitoring program capable of providing timely detection of a change in water quality that could indicate a release has occurred?
   ◯ Yes ◯ No

8. Do authorities with responsibility for upstream contamination events have effective response plans to contain spills prior to contaminating the intake?
   ◯ Yes ◯ No

Systems with a Groundwater Source

9. Does the utility have multiple sources of drinking water, such that if one were contaminated, the other(s) could be used to supply the system?
   ◯ Yes ◯ No

10. Is the utility's groundwater aquifer confined or protected from infiltration?
    ◯ Yes ◯ No

11. Is the utility's groundwater protection area relatively pristine and free of significant sources of potential contamination (as listed in Question #3, above)?
    ◯ Yes ◯ No

12. In the event of a spill, release, or other source of contamination, are there procedures for timely removal of contaminated soil and other measures to prevent contamination of the utility's aquifer?
    ◯ Yes ◯ No

Systems that Buy Water from Wholesaler Water Suppliers

13. Is information available from the supplier with respect to water source, potential contamination threats, and testing and monitoring?
    ◯ Yes ◯ No

14. Does the supplier proactively manage potential risks to their water supply?
    ◯ Yes ◯ No

15. Is there a procedure for the utility to receive timely notification of potential contamination incidents in the purchased water?
    ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
EPA *Online Water Quality Monitoring Resources*	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources	11
Local Emergency Planning Committees (LEPC) and Local Emergency Management Agencies/Directors	https://www.epa.gov/epcra	20
Envirofacts	https://www3.epa.gov/enviro/	21
EPA *Conducting Source Water Assessments*	https://www.epa.gov/sourcewaterprotection/conducting-source-water-assessments	22
Drinking Water Mapping Application to Protect Source Water	https://www.epa.gov/sourcewaterprotection/drinking-water-mapping-application-protect-source-waters-dwmaps	23
EPA Toxics Release Inventory	https://www.epa.gov/toxics-release-inventory-tri-program	24
National Response Center	https://www.epa.gov/emergency-response/national-response-center	25

Notes

1.
2.
3.
4.
5.
6.
7.
8.

Notes

9.
10.
11.
12.
13.
14.
15.

Table 13: Threat Category: Contamination of Source Water – Intentional

Threat Category Definition: *An intentional incident of contamination of a drinking water source that could result in contaminated water entering the utility. Applies to surface and groundwater sources (including purchased). The contamination may occur outside the control of the utility.*

Crosslink to AWWA J100-10 Standard Reference Threat Scenarios	Annual Default Threat Likelihood	
	Water	Wastewater
Intentional contamination of source water is not included in the J100-10 Standard.	10^{-6}	N/A
	Basis: • Estimate 100,000 utility targets in the United States. • A few incidents of intentional contamination of drinking water sources have been reported in the United States and foreign countries. • Available intelligence (public) indicates awareness and intent by terror groups and malicious individuals to carry out this type of attack. • No public health or economic impacts from this type of incident in the United States have been reported. Potential impacts would be mitigated by dilution, water treatment, and other factors. • **Conservative estimate of threat likelihood:** One attack per year among 100,000 water utilities, and 10% of attacks have the potential for significant public health or economic consequences.	

Factors for Modifying Default Threat Likelihood[15]

Systems with a Surface Water Source

1. Does the utility have multiple intakes at different locations that could be operated to prevent contamination at the site of any single intake from entering the treatment facility?
   ◯ Yes ◯ No

2. If a secured source water reservoir is used, does it have robust access control (e.g., fencing or other physical barriers) to deter or delay unauthorized access?
   ◯ Yes ◯ No

3. If a secured source water reservoir is used, is active monitoring (remote or onsite) conducted to detect unauthorized access?
   ◯ Yes ◯ No

4. Does the utility conduct real-time monitoring of source water intake locations to detect unauthorized access or tampering?
   ◯ Yes ◯ No

[15] Questions 13 – 15 are also included in the *Threat Category: Contamination of Source Water – Accidental.*

5. Does the utility have procedures in place for responding when unauthorized access or tampering is detected at source water reservoirs or intakes (if applicable)?
   ◯ Yes ◯ No

6. Is the utility's source water reservoir or intake (as applicable) easily accessible by boat or land?
   ◯ Yes ◯ No

7. Does the utility have a source water quality monitoring program capable of providing timely detection of a change in water quality that could indicate a contamination incident has occurred?
   ◯ Yes ◯ No

Systems with a Groundwater Source

8. Does the utility have multiple wells at different locations that could be operated to prevent contamination at the site of any single well from entering the treatment or distribution facility?
   ◯ Yes ◯ No

9. Would the condition of the well impede the influx of a contaminant? (For example, well depth, well condition, and soil type could impact the flow of a contaminant into the well.)
   ◯ Yes ◯ No

10. Does the wellfield have robust access control (e.g., fencing or other physical barriers) to deter or delay unauthorized access?
    ◯ Yes ◯ No

11. Is the wellfield monitored to detect unauthorized access or tampering?
    ◯ Yes ◯ No

12. Is a large-scale intentional release of contaminants in the vicinity of the wellfield feasible (e.g., are chemicals stored in proximity to an accessible wellfield)?
    ◯ Yes ◯ No

Systems that Buy Water from Wholesaler Water Suppliers

13. Is information available from the supplier with respect to water source, potential contamination threats, and testing and monitoring?
    ◯ Yes ◯ No

14. Does the supplier proactively manage potential risks to their water supply?
    ◯ Yes ◯ No

15. Is there a procedure for the utility to receive timely notification of potential contamination incidents in the purchased water?
    ◯ Yes ◯ No

Resources - see Section 5 for resource descriptions		
Resource	**Web Link**	**# in Section 5**
ASCE, *Guidelines for the Physical Security of Water Utilities* (56-10) *and Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (57-10)	https://ascelibrary.org/doi/book/10.1061/9780784411261	1
AWWA G430-14 *Security Practices for Operation and Management*	https://www.awwa.org/Store/Product-Details/productId/45320372	2
Domestic Security Alliance Council	https://www.dsac.gov/	3
InfraGard	https://www.infragard.org/	4
Local Law Enforcement Agencies	N/A	5
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers	6
Water Information Sharing and Analysis Center	https://www.waterisac.org/	7
EPA *Online Water Quality Monitoring Resources*	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources	11
EPA *Resources to Design and Implement Enhanced Security Monitoring for Surveillance and Response Systems*	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-enhanced-security-monitoring-surveillance	13

Notes

1.
2.
3.
4.
5.
6.
7.
8.

Notes

9.
10.
11.
12.
13.
14.
15.

Section 5: Resources for Additional Information

Table 14 provides additional information about the resources listed earlier for each threat category.

Table 14: Threat Category Resource Descriptions

Listing #	Resource	Description	Web Link
1	*ASCE, Guidelines for the Physical Security of Water Utilities* (56-10) *and Guidelines for the Physical Security of Wastewater/ Stormwater Utilities* (57-10)	Guidelines apply to the physical security of facilities with potable water source, treatment, and distribution systems, as well as with wastewater collection and treatment systems and stormwater systems. Provides direction for utilities as they design or retrofit their infrastructure to ensure the physical security of water and wastewater/stormwater systems. Recommendations include the use of physical and electronic security measures. (requires purchase)	https://ascelibrary.org/doi/book/10.1061/9780784411261
2	AWWA G430-14 *Security Practices for Operation and Management*	Describes criteria for a security program for a water, wastewater, or reuse utility. Includes security culture, roles and employee expectations, vulnerability assessment, dedicated resources, access control and intrusion detection, contamination detection, monitoring and surveillance, and information protection. Additionally, the standard covers design and construction, threat level-based protocols, emergency response and recovery plans and business continuity plans, internal and external communications, partnerships, documentation, human resources, and equipment. (requires purchase)	https://www.awwa.org/Store/Product-Details/productId/45320372
3	Domestic Security Alliance Council	The Domestic Security Alliance Council is a partnership between the U.S. government and the U.S. private industry that promotes the timely exchange of security and intelligence information. DSAC advances the FBI's mission of detecting, preventing, and deterring criminal acts by facilitating relationships among its private sector member companies, FBI Headquarters, FBI field offices, DHS Headquarters and Fusion Centers, and other federal government entities. DSAC also expands the U.S. private sector's ability to protect its employees, assets, and information by providing access to security information and experts, as well as continuing education for security officers.	https://www.dsac.gov/

Listing #	Resource	Description	Web Link
4	InfraGard	InfraGard is a partnership between the FBI and members of the private sector that promotes information exchange relevant to the protection of critical infrastructure. InfraGard has 82 chapters and over 46,000 members nationwide. Chapter meetings are led by a local governing board and an FBI agent who serves as InfraGard coordinator. They provide an opportunity to share information on threats and best practices.	https://www.infragard.org
5	Local Law Enforcement Agencies	Local police, county/city sheriffs, and state police maintain crime databases and can provide situational awareness of the local threat environment. Local crime information may be relevant to assessing physical threats like assault, theft, or sabotage. Also, local law enforcement can collaborate with outside law enforcement agencies like the FBI.	Search by locality
6	State and Major Urban Area Fusion Centers	State and Major Urban Area Fusion Centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners.	https://www.dhs.gov/state-and-major-urban-area-fusion-centers
7	Water Information Sharing and Analysis Center (WaterISAC)	WaterISAC is an all-threats security information source for the water and wastewater sector. It is the information sharing and operations arm of the Water Sector Coordinating Council, as authorized under the 2002 Bioterrorism Act, and provides comprehensive information on malevolent acts, including cybercrime. WaterISAC is operated by the Association of Metropolitan Water Agencies and managed by water utility managers and state drinking water administrators.	https://www.waterisac.org/
8	AWWA M-14 *Backflow Prevention and Cross Connection Control: Recommended Practices*	Provides general guidance on developing, operating, and maintaining a cross-connection control and backflow prevention program. Includes discussions on assessing the risks and preventing backflow, as well as backflow prevention assembly, application, installation, and maintenance; health and legal concerns; and detailed information on potential and real hazards.	https://www.awwa.org/Store/Product-Details/productId/46494412

Listing #	Resource	Description	Web Link
9	AWWA G200-15 *Distribution Systems Operation and Management*	Describes the operation and management of potable water distribution systems, including maintenance of water quality, system management programs, operation and maintenance of facilities, and verification.	https://www.awwa.org/Store/Product-Details/productId/49065093
10	EPA's *Cross Connection Control Manual*	Provides guidance to drinking water utilities on designing, implementing, and managing a backflow prevention program in the distribution system.	https://www.epa.gov/sites/production/files/2015-09/documents/epa816r03002_0.pdf
11	EPA *Online Water Quality Monitoring Resources*	Includes a series of guidance documents that cover the performance, design, installation, and operation of real-time water quality monitoring systems that can be used to optimize treatment processes, detect source water contamination incidents, and monitor threats to long-term water quality.	https://www.epa.gov/waterqualitysurveillance/online-water-quality-monitoring-resources
12	National Academy of Sciences *Drinking Water Distribution Systems: Assessing and Reducing Risks*	Identifies strategies to reduce the risks posed by water-quality deteriorating events in distribution systems, including backflow events via cross connections, contamination during construction and repair, and maintenance of storage facilities. The report also identifies advances in detection, monitoring and modeling, and analytical methods. (requires purchase)	https://www.nap.edu/catalog/11728/drinking-water-distribution-systems-assessing-and-reducing-risks
13	EPA *Resources to Design and Implement Enhanced Security Monitoring for Surveillance and Response Systems*	These products support the design, implementation, and commissioning of Enhanced Security Monitoring at utility distribution system facilities that are determined to be at risk of intentional contamination.	https://www.epa.gov/waterqualitysurveillance/resources-design-and-implement-enhanced-security-monitoring-surveillance
14	AWWA *Process Control System Security Guidance for the Water Sector* and Use-Case Tool	Provides a water sector-specific approach to implementation of controls in the NIST Cybersecurity Framework, and aids water systems in their prioritization of controls necessary to manage cybersecurity risks.	https://www.awwa.org/Resources-Tools/Resources/Cybersecurity-Guidance
15	DHS National Cybersecurity and Communications Integration Center	Has the lead responsibility within the federal government to assist all critical infrastructure sectors, including water, with cybersecurity. Provides threat alerts, offers tools and guidance to identify vulnerabilities, and assists with response and recovery.	https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center

Listing #	Resource	Description	Web Link
16	NIST Cybersecurity Framework	Consists of voluntary standards, guidelines, and best practices to manage cybersecurity-related risk. Focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of an organization's risk management processes.	https://www.nist.gov/cyberframework
17	NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*	Describes security and privacy controls for information systems and organizations and a process for selecting controls to protect organizational operations and assets from cyber-attacks. These controls are applicable to non-federal networks as well.	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
18	NIST SP 800-82 Revision 2, Guide to Industrial Control Systems Security	Provides guidance on how to improve security in Industrial Control Systems, including Supervisory Control and Data Acquisition systems, Distributed Control Systems, and Programmable Logic Controllers, while addressing unique performance, reliability, and safety requirements. Offers an overview of typical system topologies, identifies threats and vulnerabilities, and recommends security controls.	https://www.csiac.org/reference-doc/nist-sp-800-82-revision-2-guide-to-industrial-control-systems-ics-security/
19	WaterISAC 15 *Cybersecurity Fundamentals for Water and Wastewater Utilities*	Identifies and explains the critical elements of cybersecurity at water sector facilities. Developed by WaterISAC to address vulnerabilities identified in cybersecurity incidents and assessments. Recommentations link to corrresponding technical resources (also see Resource Listing #7).	www.waterisac.org/fundamentals
20	Local Emergency Planning Committees (LEPC) and Local Emergency Management Agencies/Directors	Under the Emergency Planning and Community Right-to-Know Act (EPCRA), Local Emergency Planning Committees (LEPCs) must develop an emergency response plan, review the plan at least annually, and provide information about chemicals in the community to citizens. There is one LEPC for each of the more than 3,000 designated local emergency planning districts. To find your LEPC, contact your local State Emergency Response Commission (SERC). AWIA requires the SERC to notify the drinking water primacy agency of any reportable releases and to provide community water systems with hazardous chemical inventory data.	https://www.epa.gov/epcra

Listing #	Resource	Description	Web Link
21	Envirofacts	Envirofacts is a searchable compendium of databases for a variety of environmental monitoring programs related to air, water, and land. It allows users to search multiple environmental databases for facility information, including toxic chemical releases, water discharge permit compliance, hazardous waste handling processes, Superfund status, and air emission estimates.	https://www3.epa.gov/enviro/
22	EPA *Conducting Source Water Assessments*	Provides information on how to determine the vulnerability of the water supply to contamination. Source water assessments are reports developed by states to help local governments, water utilities, and others protect sources of drinking water.	https://www.epa.gov/sourcewaterprotection/conducting-source-water-assessments
23	Drinking Water Mapping Application to Protect Source Water	This is an online mapping tool that helps states and drinking water utilities to update their source water assessments and protection plans. Provides locations of potential sources of contamination and polluted waterways, as well as information on protection projects and Source Water Collaborative initiatives.	https://www.epa.gov/sourcewaterprotection/drinking-water-mapping-application-protect-source-waters-dwmaps
24	EPA Toxics Release Inventory	Provides a resource for learning about toxic chemical releases and pollution prevention activities reported by industrial and federal facilities. Utilities can review information in this system to evaluate the threat posed by an accidental toxic chemical release that could impact their source water.	https://www.epa.gov/toxics-release-inventory-tri-program
25	National Response Center	The National Response Center is staffed 24 hours a day by the U.S. Coast Guard and is the designated federal point of contact for reporting all oil, chemical, radiological, biological and etiological discharges into the environment, anywhere in the United States and its territories. Reports to the NRC activate the National Contingency Plan and the federal government's response capabilities. Reports of all releases and spills are available in a national database.	https://www.epa.gov/emergency-response/national-response-center

References

American Water Works Association. (2013). *Risk and Resilience Management of Water and Wastewater Systems,* J100-10 (R13).

America's Water Infrastructure Act of 2018, Pub. L. No. 115-270, S. 3021, 115th Cong.

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

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