CONFIDENTIAL

DO NOT COPY

DO NOT RELEASE FOR PUBLIC REVIEW

Vulnerability Assessment

for

Public Water System Name:

_____

Public Water System I.D. Number:

NY _____

Prepared by: _____

Title: _____

Signature: _____

Date Completed: _____

Confidential Information "This report may contain information that if disclosed could endanger the life or safety of the public, and therefore, pursuant to section seven hundred eleven of the executive law, this report is to be maintained and used in a manner consistent with protocols established to preserve the confidentiality of the information contained herein in a manner consistent with law."

Change Log

Date	Changes Made By	Changes Made

Distribution List

Copy ID	Recipient	Distributed By	Date

TABLE OF CONTENTS

SECTION I - INTRODUCTION

This assessment contains sensitive information that must be secured from unauthorized disclosure

The following self-assessment template was developed jointly by the New York State Department of Health (NYSDOH) and the New York State Division of Homeland Security and Emergency Services (DHSES) to assist community water systems (CWS) which serve populations greater than 3,300 to identify vulnerabilities to emergencies caused by malevolent acts and natural hazards.

Previous versions of this template were developed by NYSDOH based upon documents prepared by the Association of State Drinking Water Administrators, the U.S. Environmental Protection Agency (U.S. EPA), the U.S. EPA Drinking Water Academy, the National Rural Water Association, and the New York Rural Water Association.

This 2022 update incorporates new material for cybersecurity, America's Water Infrastructure Act of 2018 (AWIA) compliance and components derived from the U.S. EPA Vulnerability Self-Assessment Tool (VSAT).

New York State Public Health Law (PHL) Section 1125 requires all community water systems serving more than 3,300 people to prepare a water supply emergency plan (WSEP). Amendments made to PHL Section 1125 in 2002 and 2017 require that the vulnerability assessment component of the WSEP include an analysis of vulnerability to terrorist attack and cyberattack. Several counties within New York have extended emergency planning requirements to other systems. Consult your local health department for any additional requirements.

Under New York State Executive Law Article 26, Section 711-B, DHSES is required to review vulnerability assessments prepared by a CWS pursuant to Public Health Law Section 1125. DHSES will utilize the information provided in the assessment to provide recommendations and general guidance based on the assessment and known risks to the water sector to enhance protections against a terrorist attack or cyberattack.

Section 2013 of AWIA requires CWS serving populations greater than 3,300 persons to conduct an assessment of the risks to and resilience of its system, termed a Risk and Resiliency Assessment or RRA. This template is intended to meet the requirements of the AWIA RRA and the requirements of NYS PHL.

This self-assessment template will help water systems identify vulnerabilities to emergencies caused by natural hazards such as floods and power outages, and vulnerabilities to malevolent acts such as terrorism and cyberattacks. When the tables provided in Sections II through VIII are completed this document will identify:

- assets of the water system and single points of failure,
- risk to system components from natural hazards and malevolent acts, and
- corrective actions that can improve security and resilience to reduce risk.

As required by Public Health Law Section 1125, the following law enforcement agencies were consulted in the process of completing this vulnerability assessment:

Section 2013 of the America's Water Infrastructure Act of 2018 requires community water systems to coordinate with existing local emergency planning committees (LEPC) to the extent possible when preparing or revising a risk and resilience assessment or an emergency response plan. LEPC contact information is available from the NYS Division of Homeland Security and Emergency Services: https://www.dhses.ny.gov/planning/serc/.

The water supply emergency plan, including this vulnerability assessment and the accompanying emergency response plan, was prepared or revised in coordination with the following LEPC:

A vulnerability assessment is a required component of a water supply emergency plan, but alone is not a complete water supply emergency plan as defined by New York State Public Health Law §1125. For security reasons, the vulnerability assessment must be kept physically separate from the rest of the water supply emergency plan.

Some key terms have been defined in a separate Appendix to this document.

SECTION II - WATER SYSTEM INFORMATION

Community Water System Name: _____

Community Water System ID: NY _____

Address: _____

County: _____

Total Population Served: _____

Average Daily Demand (MGD): _____

Primary Point of Contact:

Name: _____

Title: _____

Phone: _____

Email: _____

Alternate Point of Contact: _____

Name: _____

Title: _____

Phone: _____

Email: _____

Cybersecurity Point of Contact (if different from the above):

Name: _____

Title: _____

Phone: _____

Email: _____

SECTION III – UTILITY RESILIENCE

The questions in this section will help you assess your capability to respond to and recover from an incident that impacts critical operations.

For each question, please select the statement that best describes your circumstance. If you have any comments about your answer, please use the space at the end of this section.

1. Select the statement(s) below that best describes your emergency response plan (ERP):
   - ☐ No ERP or ERP status unknown
   - ☐ An ERP has been developed
   - ☐ Staff have been trained on the ERP (e.g., Tabletop Exercises)
   - ☐ Resource typed assets/teams defined and inventoried
   - ☐ Functional exercises on the ERP have been conducted

2. Select the statement(s) below that best describes the level to which national incident management system (NIMS) and incident command system (ICS) training has been provided to staff:
   - ☐ No ICS/NIMS training completed or ICS/NIMS training status unknown
   - ☐ ICS 100/200 provided to key staff
   - ☐ ICS 700/800 provided to key staff
   - ☐ ICS 300/400 provided to key staff
   - ☐ Utility certified as NIMS compliant*

     (*NIMS compliance is a requirement for some federally funded grants)

3. Select the statement(s) below that best describes any mutual aid and assistance (MAA) agreements into which you have entered:
   - ☐ No agreements established or MAA status unknown
   - ☐ Intra-municipal (within own city/town/village agencies)
   - ☐ Local-Local (with adjacent city/town/village)
   - ☐ Intrastate (e.g., water and wastewater agency response network (WARN))
   - ☐ Intrastate and interstate (e.g., WARN and cross-border agreement)

4. Select the statement below that best describes the length of time critical operations can be provided using backup-power without additional resources:
   - ☐ No backup power or backup power status unknown
   - ☐ Up to 24 hours of backup power
   - ☐ 25 hours to 48 hours of backup power
   - ☐ 49 hours to 72 hours of backup power
   - ☐ Greater than or equal to 73 hours of backup power

5. Select the statement below that best describes the amount of time average day demand can be provided using storage only:
   - ☐ No ability or ability unknown
   - ☐ Up to 24 hours
   - ☐ 25 hours to 48 hours
   - ☐ 49 hours to 72 hours
   - ☐ Greater than or equal to 73 hours

6. Select the statement below that best describes the lead time for repair, replacement or recovery of critical parts or equipment:
   - ☐ 3 – 4 weeks or greater, or lead time is unknown
   - ☐ 1 week to less than 3 weeks
   - ☐ 3 days to less than 7 days
   - ☐ 1 day to less than 3 days
   - ☐ Less than 24 hours

7. Select the statement below that best describes the percentage of response-capable staff who are cross-trained in critical operations and maintenance positions and available as staff backup:
   - ☐ Less than 10% or unknown
   - ☐ 10 to 25%
   - ☐ Greater than 25 to 50%
   - ☐ Greater than 50 to 75%
   - ☐ Greater than 75 to 100%

8. Select the statement below that best describes your development of a business continuity plan (BCP) to address the potential financial effects of a crisis, as well as your flexibility to adapt human resource policies to meet the changing needs of employees:
   - ☐ No BCP or unknown
   - ☐ BCP under development
   - ☐ BCP completed
   - ☐ BCP fully implemented
   - ☐ Annual commitment of resources to BCP and BCP is exercised

9. Select the statement below that best describes your operations and maintenance (O&M) manual:
   - ☐ No O&M Manual exists
   - ☐ O&M Manual is under development
   - ☐ O&M Manual is completed
   - ☐ O&M Manual is fully Implemented
   - ☐ O&M Manual is fully implemented and reviewed and updated regularly

10. Select the statement below that best describes your standard operating procedures (SOP):
    - ☐ No SOP in place
    - ☐ SOP under development
    - ☐ SOP is completed
    - ☐ SOPs is fully implemented
    - ☐ SOPs is fully implemented, all employees are trained on them, and they are reviewed and updated regularly

Use this space to provide an additional information about the answers provided to the questions above:

SECTION IV – WATER SYSTEM ASSETS

Use the table below to help characterize and identify your critical system assets. Once you have identified and prioritized assets that are essential to system operation you can develop an effective preparedness strategy.

A single point of failure is a particularly vulnerable component that if debilitated, could result in significant disruption to one or more critical missions. Single points of failure typically exist where there is inadequate or no redundancy. Add rows to the table as needed to incorporate all critical system assets.

Source Water			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Ground Water			☐
			☐
			☐
			☐
			☐
			☐
Surface Water			☐
			☐
			☐
Purchased			☐
			☐
			☐
Sold			☐
			☐
			☐

Raw Water Intakes, Pipes and Conveyances			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Intakes, Raw Water Transmission Mains, Raw Water Storage			☐
			☐
			☐
			☐
Pumps			☐
			☐
			☐
			☐
Treatment			
Buildings			☐
			☐
			☐
Pumps			☐
			☐
			☐
			☐
Treatment Equipment (e.g., flocculator, basin, filter, disinfection, fluoridation, clearwell)			☐
			☐
			☐
			☐
			☐

Use, Storage and Handling of Chemicals			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Treatment Chemical Use and Storage			☐
			☐
			☐
			☐
Laboratory Chemical Use and Storage			☐
			☐
			☐
			☐
Storage			
Ground Storage Tanks			☐
			☐
			☐
			☐
Elevated Storage Tanks			☐
			☐
			☐
			☐
Pressure Tanks			☐
			☐

Distribution System			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Pumps and Pump Stations			☐
			☐
			☐
Transmission Mains (including exposed crossings)			☐
			☐
			☐
Water Mains			☐
			☐
			☐
Valves			☐
			☐
			☐
Booster Chlorination Stations			☐
			☐
			☐
Interconnections to Other Water Systems			☐
			☐
			☐
Important Service Connections (hospitals, power plants, etc.)			☐
			☐
			☐
Appurtenances (air relief, backflow preventers, meters, etc.)			☐
			☐
			☐

Monitoring Practices			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Sensors, meters, laboratory equipment			☐
			☐
			☐
			☐
Data management equipment and systems			☐
			☐
			☐
			☐
Operations and Maintenance			
Storage of Spare Parts and Equipment			☐
			☐
			☐
			☐
Transportation and Work Vehicles			☐
			☐
			☐
			☐
Power			
Primary Power			☐
			☐
			☐
Auxiliary Power			☐
			☐
			☐

Electronic, Computer, or Other Automated Systems			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Process Control (PLC, SCADA, other electronic control or monitoring equipment)			☐
			☐
			☐
			☐
Business Enterprise Systems (meter reading, administrative, internet, email)			☐
			☐
			☐
			☐
Personnel and Offices			
Personnel			☐
			☐
			☐
Buildings			☐
			☐
			☐
Files			☐
			☐
Communications			
Telephone			☐
			☐
Cell Phone			☐
			☐
Radio			☐
			☐

Financial Infrastructure			
Component	**Number/ Size /Location (if applicable)**	**Description**	**Single Point of Failure?** (Check if Yes)
Billing, Payment and Accounting Systems			☐
			☐
			☐
Third-party Service Provider			☐
			☐
			☐
Physical Barriers			
Fences, Bollards, Perimeter Walls and Gates			☐
			☐
			☐
			☐
Locks, Card Readers, Hardened Doors, Equipment Cages			☐
			☐
			☐
			☐

SECTION V – Critical Asset Vulnerabilities

This section will help identify your system vulnerabilities by determining the risk to the asset categories and individual assets you identified in the previous section. Risk is the combination of threat, asset vulnerability and system consequence:

> **Threat**: A specific event which could impair system operation.
> **Vulnerability**: The likelihood that a threat, if it occurs, will damage, or impair an asset.
> **Consequence**: The adverse impact to the system when a threat occurs which damages or impairs the operation of an asset.

Identifying emergency conditions which are likely to occur and are likely to have a significant impact on your system operations will help identify where corrective actions are needed to reduce the risk to your system.

1. Threat Likelihood

In the following two tables indicate how likely each type of emergency is to occur.

Natural Hazards	**Probability of Occurrence**				
	Very High (Frequent)	High (Occasional)	Moderate (Seldom)	Low (Unlikely)	Very Low (Improbable)
Power outage					
Prolonged water outage					
Transmission or distribution system failure					
Pump failure					
Drought					
Flood					
Tornado					
Hurricane					
Earthquake					
Ice storm					
Fire at water supply facility					
Fire in community					
Chemical incident in facility					
Supply chain shortages					
Pandemic					
Other (specify):					

Malevolent Acts	Probability of Occurrence				
	Very High (Frequent)	High (Occasional)	Moderate (Seldom)	Low (Unlikely)	Very Low (Improbable)
Assault on utility – physical					
Theft or diversion – physical					
Sabotage – physical					
Vandalism					
Contamination of water source (intentional or unintentional)					
Contamination of finished water (intentional or unintentional)					
Cyberattack on process control system or SCADA					
Cyberattack on business enterprise system					
Terrorist attack					
Other (specify):					

2. Risk Assessment

In the following tables you will assess the risk posed to your system by the moderate to very high probability natural hazards and malevolent acts you identified in the previous section. For each emergency, first identify the components of your system that have a high probability of being affected by the emergency condition. Focus on emergency conditions that are likely to occur (threat) and are likely to impact a system asset or component (vulnerability). This will help you focus on those system components that, if damaged, would significantly impair the operation of your system (consequence).

For emergency conditions which pose a significant risk to the normal operation of your system, you will need to identify corrective actions to reduce risk. Corrective actions should reduce the vulnerability of your assets to that emergency condition or reduce the consequence to your system should the asset be impacted.

Complete the following tables for each emergency condition. An example of a completed table is provided.

Emergency: Flood (Example)

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☒ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☒ Pumps and pump stations
- ☐ Transmission mains
- ☒ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☒ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date this action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page: Pump Station		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity: Will be unable to pump water to high service area. High service will run out of water once tank is depleted.	
Mitigation	Proposed Corrective Action: Move pumps and electronics above flood level	
	Priority (High/Medium/Low): Medium	Target Completion Date: 2025
2. Vulnerable Critical Asset from Previous Page: Building		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity: Treatment buildings may flood and have to be shut down	
Mitigation	Proposed Corrective Action: Develop plan for securing and deploying sandbags and trash pumps	
	Priority (High/Medium/Low): High	Target Completion Date: 2024
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Power outage

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Prolonged water outage

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Transmission or distribution system failure

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Pump failure

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Drought

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Flood

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Tornado

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Hurricane

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Earthquake

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Ice storm

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Fire at water supply facility

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Fire in the community

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Chemical incident in facility

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Supply chain shortages

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Pandemic

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Terrorist attack

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Physical assault on system

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Physical theft or diversion

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Physical sabotage

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Contamination of water source (intentional or unintentional)

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Contamination of finished water (intentional or unintentional)

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Cyber attack on process control system or SCADA

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Cyberattack on business enterprise system

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Emergency: Terrorist attack

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

Other Emergency:

Check the system components that have a HIGH PROBABILITY of being affected by this emergency.

Source Water:
- ☐ Groundwater or springs
- ☐ Surface water
- ☐ Purchased
- ☐ Sold

Raw Water Intakes, Pipes, and Conveyances
- ☐ Intakes, raw water transmission mains, raw water storage
- ☐ Pumps

Treatment:
- ☐ Buildings
- ☐ Pumps
- ☐ Treatment equipment

Chemical Use, Storage, and Handling:
- ☐ Treatment chemical use and storage
- ☐ Laboratory chemical use and storage

Storage:
- ☐ Ground storage tanks
- ☐ Elevated storage tanks
- ☐ Pressure tanks

Distribution System:
- ☐ Pumps and pump stations
- ☐ Transmission mains
- ☐ Water mains
- ☐ Valves
- ☐ Booster chlorination stations
- ☐ Interconnections to other water
- ☐ Important service connections
- ☐ Appurtenances

Monitoring Practices:
- ☐ Sensors, meters, laboratory equipment
- ☐ Data management equipment and systems

Operations and Maintenance:
- ☐ Storage of spare parts and equipment
- ☐ Transportation and work vehicles

Power:
- ☐ Primary power
- ☐ Auxiliary power

Electronic, Computer, or Other Automated Systems:
- ☐ Process control
- ☐ Business enterprise systems

Personnel and Office:
- ☐ Personnel
- ☐ Buildings
- ☐ Records, files, and maps

Communications:
- ☐ Telephone
- ☐ Cell phone
- ☐ Radio

Financial Infrastructure:
- ☐ Billing, payment, and accounting systems
- ☐ Third-party service provider

Physical Barriers
- ☐ Fences, bollards, perimeter walls and gates
- ☐ Locks, card readers, hardened doors, and equipment cages

☐ **No components have a high probability of being impacted.**
Continue to next emergency.

Threat	Does this emergency have a moderate, high, or very high probability of occurring? (Refer to your threat probability assessment on pages 14-15):	☐ Yes ☐ No
If Yes, complete the rest of the table:		
Vulnerability	Review the system assets you identified as vulnerable on the previous page and enter below the most critical assets which, if impacted by this emergency, would significantly impair the operation of your system. For each asset, propose a corrective action which would reduce the risk to the asset or your system. Provide the priority and completion date for action. Use additional sheets if more than three critical assets were identified. Check the box below and continue to the next emergency if no critical assets were identified.	
	☐ No critical assets identified. System will be able to operate at normal capacity with the identified assets unable to operate due to impacts from this emergency.	
1. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset becomes non-operational or is only able to operate at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
2. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:
3. Vulnerable Critical Asset from Previous Page:		
Consequence	Describe the impact to your system if this asset was non-operational or operating at a reduced capacity:	
Mitigation	Proposed Corrective Action:	
	Priority (High/Medium/Low):	Target Completion Date:

SECTION VI - SECURITY AND OPERATIONS

The questions in this section will help identify potential security and operational vulnerabilities. Include all your potentially vulnerable infrastructure even if it has not been identified as a critical asset.

Some of the questions have been mapped back to components of Best Practices for Anti-Terrorism Security (BPATS) for Commercial Office Buildings. The BPATS Assessment Tool for Commercial Facilities is a program for evaluating a building's security system. It contains components which consist of standards, guidelines, and practices to promote the protection of critical infrastructure. Additional information on BPATS can be found here: https://bpatsassessmenttool.nibs.org/

Please select the best answer to each question. If your answer is No, include a corrective action and a target completion date. If you answer not applicable (N/A), explain why this is so for your facility.

1. Is access to all components of your water system restricted to authorized personnel only? *(3.2 Identification and Verification -3.2.01-3.2.08)*
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

2. Are warning signs (tampering, unauthorized access, etc.) posted on all components of your water system, e.g., storage tanks, well houses and other buildings? *(5.2 Signage and Announcements - 5.2.07)*
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

3. Do you have emergency contact information posted at all water system locations? *(5.2 Signage and Announcements - 5.2.07)*
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

4. Are fences and gates or other perimeter security measures in place at all locations? (*4.2 Systems – Access control – Perimeter -4.2.28-4.2.34)*
    a. At your facilities (buildings, tanks, etc.)?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. At all source(s) (well heads, reservoirs, etc.)?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Are these routinely checked?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Is vehicle access to all critical components adequately restricted or otherwise controlled? (*Screening, Monitoring, Surveillance - 4.2.12-4.2.16)*
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

5. Are the following components of your system properly locked and secured or equipped with other features which delay unauthorized access? (*Access control – Screening, Monitoring, Surveillance - 4.2.12-4.2.16) and 4.2 Systems - Detecting - 4.2.01-4.2.03)*
    a. Doors, windows, and other points of human access?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

b. Roof hatches, vents, etc.?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Wellheads?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

d. Well vents and caps?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

e. Tank ladders, access hatches, and entry points?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

f. Vehicles?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

g. Areas of your water system that are exposed or vulnerable during repair or construction activities?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

h. Observation, test, and/or abandoned wells?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

i. Vents and overflow pipes?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

6. Do facilities have ample lights, easily observable assets or other features which deter unauthorized access? *(6.5 Utility Systems and Equipment - 6.5.05)*
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

7. Do facilities have alarm systems, surveillance cameras, or other features which detect unauthorized access? *(4.2 Systems - Detecting - 4.2.01-4.2.03)*
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

8. Are fire/smoke alarms provided within all structures?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

9. Can you isolate and drain to waste your water storage tanks without using any of the distribution system?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

10. Do you control the use of hydrants and valves by other parties?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

11. Does your system monitor for, and maintain, positive distribution pressure?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

12. Has your system implemented a backflow prevention program?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

13. Are all existing emergency interconnections to other water systems exercised on a regular basis?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

14. Do you monitor raw and treated water so that you can detect changes in water quality?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

15. Are chemicals, particularly those that are potentially hazardous or flammable, properly stored in a secure area?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

16. Have you discussed with your supplier(s) procedures to ensure the security and availability of their products?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

17. Are deliveries of chemicals and other supplies made in the presences of water system personnel? *(Screening, Monitoring, Surveillance - 4.2.12-4.2.16)*
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

18. Is sensitive and/or confidential information kept secure by:
    a. Labeling as CONFIDENTIAL?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Storing in a secure location?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Limiting access and returning to the water system upon completion of construction or other projects?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

19. Does your water system have a procedure to deal with public information requests, and to restrict distribution of sensitive information?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

20. When hiring personnel...
    a. Do you request local police or a third party to perform a criminal background check? *(3.2 Identification and Verification - 3.2.01-3.2.08)*
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Are background checks repeated regularly?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Do you verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

21. Does your facility...?
    a. Have a key control and accountability policy?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Ensure that entry codes and keys are limited only to personnel with need?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

22. Are personnel issued photo-identification cards and required to keep them visible?
    ☐ Yes
    ☐ No – Corrective Action:

    Target Completion Date:
    ☐ N/A – Please Explain:

23. When employees leave or are terminated, do you require personnel to turn in photo IDs, keys, access codes, and other security-related items?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

24. Have water system personnel been advised to report security concerns and suspicious activity?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

25. Do water system personnel, including those who answer phones, have a checklist to use for threats or suspicious calls or to report suspicious activity?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

26. Does your water system have procedures in place to respond immediately to a customer complaint about a new taste, odor, color, or other physical change?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

27. Do you have a procedure in place to advise the community of contamination immediately after discovery?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

28. Do you have a procedure in place to receive notification of a suspected outbreak of a disease immediately after discovery by local health agencies?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

29. Do you have a program to educate and encourage the public to be vigilant and report suspicious activity to assist in the protection of your water system? (2.2 Risk Awareness - 2.2.07) and 5.1 Policies and Procedures - 5.1.22-5.1.26)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

SECTION VII – CYBER SECURITY

Implementing cybersecurity best practices is a critical component to safeguarding a drinking water utilities ability to deliver clean, safe water. Cyberattacks are a growing threat to critical infrastructure sectors, including water systems.

The questions in the following checklist have been mapped back to components of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0) that you will find at the end of each question. It contains components which consist of standards, guidelines, and practices to promote the protection of critical infrastructure. Informative references are also provided for each component of the *Framework*. Additional information on the *Framework* is available at: https://www.nist.gov/cyberframework.

Process control systems (PCS), such as supervisory control and data acquisition (SCADA) systems, operate and monitor various functions at many water treatment, distribution and storage facilities. Examples of PCS functions include operating pumps and valves, monitoring and transmitting storage tanks levels, and recording and storing regulatory monitoring data.

Business enterprise systems encompass all other systems not used to operate and monitor water treatment and distribution. Examples include systems used for: email and internet access; customer accounts, meter reading, and billing; water system websites; and other administrative functions.

Please select the best answer to each question. If your answer is No, include a corrective action and target completion date. If you answer not applicable (N/A), explain why this is so for your facility.

1. Have PCS assets been recently inventoried (biannually or when a new item is procured), including applications, data, servers, workstations, field devices (e.g., programmable logic controllers), communications and network equipment? (ID.AM-1,ID.AM-2)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

2. Have business system assets been recently inventoried (biannually or when a new item is procured, including application`s, data, servers, workstations, field devices (e.g., meter reading equipment), communications and network equipment? (ID.AM-1,ID.AM-2)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

3. Have the critical assets of the PCS been identified? (ID.AM-5,ID.BE-5)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

4. Have the risks and benefits of completely disconnecting the PCS from each network been evaluated? (ID.RA-5, DE.AE-4)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

5. Do you have an assigned information security officer? (ID.GV-2)
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

6. Do you have a written cybersecurity policy for … (ID.GV-1)
   a. Process control systems?
      - ☐ Yes
      - ☐ No – Corrective Action:

        Target Completion Date:
      - ☐ N/A – Please Explain:

   b. Business enterprise systems?
      - ☐ Yes
      - ☐ No – Corrective Action:

        Target Completion Date:
      - ☐ N/A – Please Explain:

c. All levels of staff at the utility?
   ☐ Yes
   ☐ No – Corrective Action:

   Target Completion Date:
   ☐ N/A – Please Explain:

d. Outside entities (vendors, service providers, etc.)?
   ☐ Yes
   ☐ No – Corrective Action:

   Target Completion Date:
   ☐ N/A – Please Explain:

7. Are staff at all organizational levels and all outside entities periodically trained on … (PR.AT-1)
   a. The cyber security policy?
      ☐ Yes
      ☐ No – Corrective Action:

      Target Completion Date:
      ☐ N/A – Please Explain:

   b. Their cyber security roles and responsibilities?
      ☐ Yes
      ☐ No – Corrective Action:

      Target Completion Date:
      ☐ N/A – Please Explain:

   c. Cyber security threats?
      ☐ Yes
      ☐ No – Corrective Action:

      Target Completion Date:
      ☐ N/A – Please Explain:

8. Do you receive cyber security threat and vulnerability updates from information sharing entities such as US-CERT or WaterISAC? (ID.RA-2)
   ☐ Yes
   ☐ No – Corrective Action:

   Target Completion Date:
   ☐ N/A – Please Explain:

9. Are PCS assets physically secured from unauthorized personnel by….? (PR.AC-2)
    a. Electrical or mechanical door locks?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Guards or cameras?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Signs?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Barricades?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

10. Are business enterprise system assets physically secured from unauthorized personnel by….? (PR.AC-2)
    a. Electrical or mechanical door locks?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Guards or cameras?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

c. Signs?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

d. Barricades?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

11. Is there an updated access control list of all water system and non-water system personnel with access to the PCS? (PR.AC-1)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

12. Is there an updated access control list of all water system and non-water system personnel with access to the business enterprise system? (PR.AC-1)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

13. When personnel are no longer employed (whether terminated or resigned), or in a position where access is no longer needed, are their credentials within the systems terminated immediately? (PR.AC-1)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

14. Are PCS account privileges limited to only those privileges which are needed to complete required work? (PR.AC-4, PR.PT-3)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

15. Are business enterprise system account privileges limited to only those privileges which are needed to complete required work? (PR.AC-4, PR.PT-3)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

16. Is there a regularly updated list of all personnel with administrative privileges on the PCS? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

17. Is there a regularly updated list of all personnel with administrative privilegeson the business enterprise system? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

18. Are administrative privileges … (PR.AC-4, PR.AT-2)
    a. Limited only to dedicated administrator accounts?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Used only when carrying out administrative functions on the system?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

19. Are there restrictions on who can and cannot install software and updates? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

20. Have password policies been put in place which require… (PR.AC-1)
    a. Strong passwords (14 characters without multi-factor authentication (MFA) or 8 characters with MFA is recommended) which are changed regularly?
       ☐ Yes
       ☐ No – Corrective Action:

       Target Completion Date:
       ☐ N/A – Please Explain:

    b. Each user to have unique credentials to log in to all PCS and business enterprise systems? (PR.AC-1)
       ☐ Yes
       ☐ No – Corrective Action:

       Target Completion Date:
       ☐ N/A – Please Explain:

    c. Different log in credentials for PCS and business enterprise systems?
       ☐ Yes
       ☐ No – Corrective Action:

       Target Completion Date:
       ☐ N/A – Please Explain:

    d. Auto screen saver with password protection on all PCS? (PR.AC-1)
       ☐ Yes
       ☐ No – Corrective Action:

       Target Completion Date:
       ☐ N/A – Please Explain:

    e. Auto screen saver with password protection on all business systems? (PR.AC-1)
       ☐ Yes
       ☐ No – Corrective Action:

       Target Completion Date:
       ☐ N/A – Please Explain:

21. Is a baseline of network operations and expected data flows for users and systems established and monitored? (DE.AE-1)
    ☐ Yes
    ☐ No – Corrective Action:

    Target Completion Date:
    ☐ N/A – Please Explain:

22. Is the network monitored to detect and alert on potential cyber security incidents? *(DE.CM-1)*
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

23. Is remote access for PCS via local area network, internet, or other means, protected by… (PR.AC-3, PR.AC-5)
    a. Firewall?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Password?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Dial back protocol or VPN?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    d. Multifactor authentication?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    e. Limiting permissions to only the minimum level required, e.g., using view-only webpages instead of allowing modification to system settings remotely?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

24. Is remote access for business systems via local area network, internet, or other means, protected by… (PR.AC-3, PR.AC-5)
    a. Firewall?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Password?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Dial back protocol or VPN?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Multifactor authentication?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    e. Limiting permissions to only the minimum level required, e.g., using view-only webpages instead of allowing modification to system settings remotely?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

25. Is encryption for PCS used for… (PR.DS-1, PR.DS-2, PR.PT-4)
    a. Data transfer?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

b. Data transfer on wireless links?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Stored data?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

26. Is encryption for business systems used for… (PR.DS-1, PR.DS-2, PR.PT-4)
    a. Data transfer?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Data transfer on wireless links?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Stored data?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

27. Are physically separate computer and network systems used for PCS and business enterprise functions? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

28. Do critical systems use application allowlisting, which only allows execution of approved files, applications, and programs? (PR.AC-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

29. Has PCS equipment… (PR.AC-5, PR.PT-2)
    a. Been blocked from all non-PCS functions, including internet browsing and email access?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    b. Been blocked from other non-PCS access to remote systems or services?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    c. Had USB, DVD, and other external media ports disabled?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

    d. Had auto-scan of removable media disabled?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

30. Are mobile devices (e.g., laptops, tablets, smartphones) which are used to access or control PCS equipment … (PR.AC-3)
    a. Included in established security policies?
       - ☐ Yes
       - ☐ No – Corrective Action:

         Target Completion Date:
       - ☐ N/A – Please Explain:

b. Encrypted?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Dedicated for PCS use only with non-essential software removed and any unnecessary functions disabled?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

31. Do PCS assets … (DE.CM-4, PR.IP-12)

a. Use anti-virus and anti-malware software?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

b. Regularly update virus and malware definitions?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

c. Regularly scan storage media for viruses and malware?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

d. Install security patches on all systems regularly?
   - ☐ Yes
   - ☐ No – Corrective Action:

     Target Completion Date:
   - ☐ N/A – Please Explain:

32. Do the business enterprise systems … (DE.CM-4, PR.IP-12)
    a. Use anti-virus and anti-malware software?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Regularly update virus and malware definitions?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    c. Regularly scan storage media for viruses and malware?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    d. Install security patches on all systems regularly?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

33. For devices with memory capabilities (e.g., laptops, multi-function printers, and cell phones) are there policies in place for… (PR.DS-3, PR.IP-6)
    a. Transferring devices from one employee to another?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

    b. Removing or permanently destroying any stored data when removing devices from service?
        ☐ Yes
        ☐ No – Corrective Action:

        Target Completion Date:
        ☐ N/A – Please Explain:

34. Is an uninterruptable power supply used for control continuance on PCS? (ID.BE-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

35. Are system and data backups performed regularly? (PR.IP-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

36. Has the system recently been successfully restored using backups (quarterly is recommended)? (PR.IP-4)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

37. Has a cyber security emergency response plan been established, and has it been reviewed in the past 12 months and updated when significant changes occur? (PR.IP-9)
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

38. Have you had a cyber security audit of your system completed in the past 12 months?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain:

39. Do you regularly review your utility, local community, and other web sites for security sensitive information related to your system that could be used to disrupt your system or contaminate your water?
    - ☐ Yes
    - ☐ No – Corrective Action:

      Target Completion Date:
    - ☐ N/A – Please Explain: