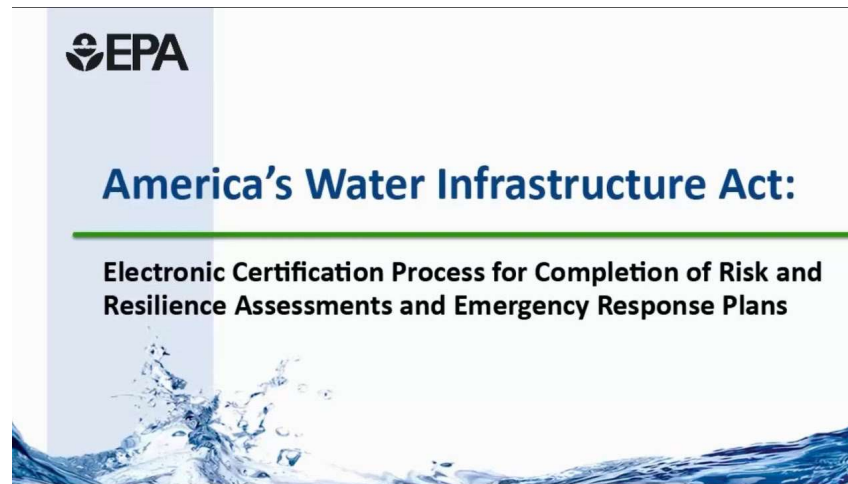


**Risk and Resiliency-  
*Creating a Comprehensive  
and Robust Emergency  
Response Plan***



# AWIA

Section 2013 of America's Water Infrastructure Act of 2018 (AWIA) requires community water systems that serve more than 3,300 people to complete a risk and resilience assessment and develop an emergency response plan.



# Available Resources



<https://www.epa.gov/waterriskassessment>




# **Community Water System Emergency Response Plan**

**Template and Instructions**






## Who Should Use this Guidance?

- This guidance is intended for small community water systems (CWSs) serving greater than 3,300 but less than 50,000 people to comply with the requirements for **risk and resilience assessments** under *America's Water Infrastructure Act of 2018 (AWIA)*.
  - For larger CWSs, EPA recommends the [Vulnerability Self-Assessment Tool \(VSAT\) Web 2.0](#) or an alternate risk assessment method.
  - CWSs serving 3,300 or fewer people are not required to conduct risk and resilience assessments under AWIA. EPA recommends, however, that very small CWSs use this or other guidance to learn how to conduct risk and resilience assessments and address threats from malevolent acts and natural hazards that threaten safe drinking water.
- 



## What is the Purpose of this Guidance?


- This guidance will help small CWSs meet the requirements for risk and resilience assessments in AWIA.
  - This guidance does not address emergency response plans (ERPs), which are also required under AWIA for CWSs serving more than 3,300 people.
    - EPA has developed an [Emergency Response Plan Template and Instructions](#) for CWSs to comply with AWIA.
  - Further, this guidance does not cover all aspects of water system security and resilience, such as asset management, climate change, and emergency preparedness and response. Visit EPA's [Drinking Water and Wastewater Resilience](#) page to find more information.
- 



## What are the Risk and Resilience Assessments Requirements in AWIA?

AWIA requires CWSs serving more than 3,300 people to assess the risks to and resilience of the system to malevolent acts and natural hazards. The law specifies water system assets (e.g., infrastructure) that the assessment must address. These assets are listed in Tables 1a – 10b in the *Risk and Resilience Assessment Checklist* (see fillable checklist below on page 4).

Water systems **must certify to EPA** that the system conducted the assessment not later than the following dates:

- March 31, 2020 for systems serving 100,000 or more
  - December 31, 2020 for systems serving 50,000 or more but less than 100,000
- 

## What are Risk and Resilience in a Water System?

- **Risk** to critical infrastructure, including water systems, is a function of **threat likelihood**, **vulnerability**, and **consequence**.
  - **Threat** can be a malevolent act, like a cyberattack or process sabotage, or a natural hazard, such as a flood or hurricane.
  - **Threat likelihood** is the probability that a malevolent act will be carried out against the water system or that a natural hazard will occur.
  - **Vulnerability** is a weakness that can be exploited by an adversary or impacted by a natural hazard. It is the probability that if a malevolent act or a natural hazard occurred, then the water system would suffer significant adverse impacts.
  - **Consequences** are the magnitude of loss that would ensue if a threat had an adverse impact against a water system. Consequences may include:
    - Economic loss to the water system from damage to utility assets;
    - Economic loss to the utility service area from a service disruption, and
    - Severe illness or deaths that could result from water system contamination, a hazardous gas release, or other hazard involving the water system.
- **Resilience** is the capability of a water system to maintain operations or recover when a malevolent act or a natural hazard occurs.
- **Countermeasures** are steps that a water system implements to reduce risk and increase resilience. They may include plans, equipment, procedures, and other measures.







## How does a Community Water System Assess Risk and Resilience Under AWIA?

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

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

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





2. For each malevolent act that you identify as a significant risk, briefly describe how the malevolent act could impact the asset category at the CWS. Include major assets that might be damaged or disabled, water service restrictions or loss, and public health impacts as applicable.

3. Select only the **natural hazards** from those listed in the table that may pose a significant risk to the asset category at the CWS. You may write-in natural hazards not listed in the table.

a. Focus the selection of natural hazards on those that are prevalent in the area where the water system is located, may affect vulnerable water system infrastructure, and have the potential for significant economic or public health consequences related to the CWS.


4. For each natural hazard that you identify as a significant risk, briefly describe or provide examples of how the hazard could impact the asset category at the CWS. Include major assets that might be damaged or disabled, water service restrictions or loss, and public health impacts as applicable.

**5. OPTIONAL Table 11 (*Risk and Resilience Assessment Checklist, see below*):** Identify **countermeasures** that the CWS could potentially implement to reduce risk from the malevolent acts and natural hazards that you selected in this assessment.

a. For malevolent acts, countermeasures are intended to deter, delay, detect, and respond to an attack.

b. For natural hazards, countermeasures are intended to prepare, respond, and recover from an event.

**NOTE:** A single countermeasure, such as emergency response planning or power resilience, may reduce risk across multiple malevolent acts, natural hazards and asset categories.





# Emergency Response Plan Example





### External Response Partner Roles

Name/Title	Organization	Responsibilities During an Incident
Local Partners		
	<i>County Emergency Management/EOC</i>	
	<i>911</i>	
	<i>Police</i>	
	<i>Fire/HazMat</i>	
	<i>LEPC</i>	
	<i>Elected officials</i>	
	<i>Neighboring Wastewater utility</i>	
	<i>Neighboring Water utility</i>	
	<i>Power utility</i>	
	<i>Health department</i>	
	<i>Contractor/vendor</i>	
	<i>Industry representative</i>	
	<i>Mutual aid</i>	
	<i>Other</i>	
	<i>Other</i>	

**Name/Title****Organization****Responsibilities During an Incident**

## State Partners

	<i>Primacy Agency</i>	
	<i>Health department</i>	
	<i>Police</i>	
	<i>WARN</i>	
	<i>Laboratories</i>	
	Other	
	Other	

## Federal Partners

	<i>EPA regional office</i>	
	<i>FBI field office</i>	
	<i>CDC</i>	
	Other	
	Other	



### 1.3.2 External Response Partner Communication

List all external response partners, their response role or position as well as contact information.

External Response Partner Contact List				
Organization or Department	Point Person Name or Position	Phone	Alternate Phone	Email or Website
<b>Local Partners</b>				
County Emergency Management/EOC				
911				
Police				
Fire/HazMat				
LEPC				
Elected officials				
Wastewater utility				
Water utility				
Power utility				
Health department				
Contractor/vendor				
Industry rep.				
Mutual aid				
Other				






**State Partners**

<i>Primacy agency</i>				
<i>Health department</i>				
<i>Police</i>				
<i>WARN</i>				
<i>Laboratories</i>				
<i>Other</i>				

**Federal Partners**

<i>EPA regional office</i>				
<i>FBI field office</i>				
<i>CDC</i>				
<i>Other</i>				



### 1.3.3 Critical Customer Communication

List critical customers below who should be given priority notification due to their reliance on the water supply either for medical reasons, based on usage, public health mission or because they may serve customers considered to be sensitive sub-populations.

Critical Customer Contact List					
Organization or Department	Point Person Name or Position	Contact Instructions	Phone	Alternate Phone	Email or Website
Wholesale customer					
Senior living center					
Nursing home					
Hospital					
Dialysis clinic					
Hotel					
Transportation center					
School					
University					
Daycare center					
Factory					
Government building					
Large water user					
Other					



### 1.3.4 Communication Equipment Inventory

Inventory your utility's communication equipment below.

---

Communication Equipment			
Type	Assigned to	Location	Number/Frequency/Channel

---

## 1.4 Media Outreach

List contact information for all media outlets that your utility may coordinate with during notification efforts. Additionally, include existing risk communication procedures, such as composing and delivering messages (e.g. message mapping), or reference an existing Risk Communication Plan.

Contact List				
Organization or Department	Point Person Name & Position	Phone	Alternate phone	Email or Website
<i>Utility social media coordinator</i>				
<i>Newspaper - Local</i>				
<i>Newspaper – Regional/State</i>				
<i>Radio station</i>				
<i>TV station</i>				
<i>Advertising agency</i>				
Other				
Other				

## 2.1 Core Response Procedures

Core procedures are the “building blocks” for incident specific response procedures, as they are typically implemented across a broad variety of incidents (e.g., hurricane, earthquake, flood). List all your core procedures here.

Access	
Item	Description
Debris clearing	List or reference here any supplies or equipment your utility owns to help with debris clearing; this includes safety items/personal protective equipment, chainsaws, and debris/earth moving equipment. If you do not have it, list where you will get it from.
Alternate routes	List or reference here alternate routes (e.g., if there is a bridge that connects your community, what are your travel options if the bridge becomes impassable?). If the alternate routes are too long, consider staging similar critical equipment and resources in different areas of your community.
Identification badges	Provide personnel with an official utility ID for access through police barricades or hazmat contaminated zones. If your jurisdiction has an identification program for first responders, be sure to participate.
Other	

Physical Security	
Item	Description
Access control procedures	List or reference your facility access control procedures here, such as key cards are required to access all buildings. Also, list any lockdown procedures as appropriate as well as the process for establishing a security perimeter following a major incident.
Restricted areas	List or reference any restricted areas of your facilities here, such as chemical rooms and electrical closets. Also list who may access those areas.
Evidence protection measures	Describe or reference your procedures for working with law enforcement if an incident is declared a crime scene.
Security culture	Increase organizational attentiveness to security to help reduce vulnerability and enhance preparedness. For example, a “See Something, Say Something” campaign for your utility. List measures your utility implements here.
Other	

## Cybersecurity

<b>Item</b>	<b>Description</b>
<i>Disconnect procedure</i>	<i>If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware.</i>
<i>Notification</i>	<i>List who should be called in the event of a cyber incident, such as your utility information technology (IT) supervisor or your contracted IT service provider. Also list any external entities that may have remote connections to your network.</i>  <i>Include any state resources that may be available such as State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) (888-282-0870 or NCCIC@hq.dhs.gov).</i>
<i>Assess procedure</i>	<i>Assess any damage to utility systems and equipment, along with disruptions to utility operations.</i>
<i>Implementation processes</i>	<i>Implement actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary) and provide public notification (if required).</i>
<i>Documentation</i>	<i>Include forms to document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).</i>
<i>Other</i>	

## Power Loss

<b>Item</b>	<b>Description</b>
<i>Backup power systems</i>	<i>List or reference your auxiliary power sources (fixed and portable) if you have not already done so elsewhere in your ERP. Provide a summary of critical facility power requirements, generator siting requirements, and the location and capacity of any existing on-site generators at all critical infrastructure components.</i>
<i>Power utility</i>	<i>Coordinate with your power utility for expected restoration priorities and timing. Power utility contact information should be listed in Section 3.2 above.</i>
<i>Fuel plan</i>	<i>Provide an inventory of on-site fuel supplies and list or reference your procedures to obtain additional fuel from vendors for your backup generators during an incident.</i>
<i>Maintenance plan</i>	<i>Maintaining generators during extended outages is critical. List your maintenance procedures for each generator, who is responsible for implementation and include lists of on-hand items such as spare parts and filters.</i>
<i>Other</i>	



---

### Emergency Alternate Drinking Water Supplies\*

---

<b>Item</b>	<b>Description</b>
<i>Bottled water</i>	Provider name: Phone: Contract No. (if applicable): Available supply: Distribution point (notify public of location):
<i>Bulk water (check with your state first for licensed water haulers)</i>	Provider name: Phone: Contract No. (if applicable): Available supply: Distribution point (notify public of location):

\* Interconnections are listed and described in Section 3.1

---



## Sampling and Analysis

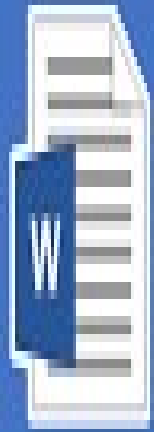
Item	Description
<i>Sampling procedures</i>	<i>Identify proper sampling procedures for different types of contaminants and attach those procedures to your ERP or reference where they can be found. Determine the quantity of required samples.</i>
<i>Pre-identified sampling locations</i>	<i>While some sampling sites will be dictated by the emergency, you can pre-plan your ideal sampling locations such as tanks and reservoirs or entry and exit points from pressure zones.</i>
<i>Sampling containers and preservatives</i>	<i>Obtain and inventory all sample containers and preservatives and list or reference them here.</i>
<i>Sample collection</i>	<i>Confirm who will be responsible for sample collection during an emergency and who can take over if that person is not available. List those names here.</i>
<i>Sample transportation</i>	<i>Confirm who will be responsible for transportation during an emergency and who can take over if that person is not available. List those names here.</i>
<i>Laboratory capabilities</i>	<i>Confirm what contaminants can be analyzed and your lab's surge sampling capacity. It may be helpful to have several backup laboratories in case your utility's lab or preferred contract lab are overwhelmed with high sample volume. Identify contract laboratories in the following table.</i>
<i>Interpreting results</i>	<i>Work with the appropriate lab, utility and regulatory agency personnel to interpret sample results. List those names here.</i>
Other	

### Local Contract/State/Federal Laboratory Contact List

Name	Address	Analytes/Methods	Phone	Email or Website
		<i>Metals, VOCs and SVOCs</i>		

### Family and Utility Personnel Well Being

Item	Description
<i>Family disaster plan</i>	<i>Implement your family plan to ensure their well-being during an incident.</i>
<i>Assembly area</i>	<i>List all the assembly areas and evacuation procedures for personnel.</i>
<i>Supplies</i>	<i>List the supplies necessary to maintain personnel health and well-being during an incident (e.g., food, potable water, cots, first aid kit, sanitary products).</i>
<i>Alternate work and shelter locations</i>	<i>Personnel may need to work from home. Or, they may need to shelter at a hotel or your utility if conditions do not permit travel home. List conditions for which work at home provisions will be triggered and list sheltering locations and procedures here.</i>
<i>Extreme temperatures</i>	<i>List or reference here any supplies or equipment your utility owns to mitigate extreme temperatures such as cold weather items (e.g., sand, salt, ice melt, tire chains, snowshoes) and hot weather items (e.g., pop-up shade canopies, water coolers, broad-brimmed hats).</i>
<i>Other</i>	



# Risk and Resilience Assessment Checklist

# Community Water System Risk and Resilience Assessment

**Enter Community Water System Name  
Risk and Resilience Assessment**

Please fill in the information below.

---

Facility Name (if applicable):

---

PWSID:

---

Analyst Name(s):

---

Date of Analysis:

---

Analysis Notes:

Enter Community Water System Name

Table 1a: Physical Barriers (Malevolent Acts)<sup>1</sup>

Asset Category: <i>Physical Barriers</i>	
Examples of Assets in this Category: Encompasses physical security in place at the CWS. Possible examples include fencing, bollards, and perimeter walls; gates and facility entrances; intrusion detection sensors and alarms; access control systems (e.g., locks, card reader systems); and hardened doors, security grilles, and equipment cages.	
Malevolent Acts	Brief Description of Impacts
Select the malevolent acts in the left column that pose a <u>significant risk</u> to this asset category at the CWS.	If you select a malevolent act in the left column as a significant risk to the <i>Physical Barriers</i> asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS. Include effects on major assets, water service, and public health as applicable.
<input type="checkbox"/> Assault on Utility – Physical	
<input type="checkbox"/> Contamination of Finished Water – Intentional	
<input type="checkbox"/> Contamination of Finished Water – Accidental <sup>2</sup>	
<input type="checkbox"/> Theft or Diversion – Physical	
<input type="checkbox"/> Cyberattack on Business Enterprise Systems	

<sup>1</sup>In a risk assessment, physical barriers are usually treated as countermeasures, which reduce the risk of a threat to an asset, rather than being treated as assets. However, under AWIA, a CWS must assess the risks to and resilience of physical barriers.

<sup>2</sup>Accidental contamination is not a malevolent act. It is included here due to similar potential consequences and because whether a contamination incident is intentional or accidental may not be known during initial response.

**Enter Community Water System Name**

Asset Category: <i>Physical Barriers</i>	
Examples of Assets in this Category: Encompasses physical security in place at the CWS. Possible examples include fencing, bollards, and perimeter walls; gates and facility entrances; intrusion detection sensors and alarms; access control systems (e.g., locks, card reader systems); and hardened doors, security grilles, and equipment cages.	
Malevolent Acts	Brief Description of Impacts
Select the malevolent acts in the left column that pose a <u>significant risk</u> to this asset category at the CWS.	If you select a malevolent act in the left column as a significant risk to the <i>Physical Barriers</i> asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS. Include effects on major assets, water service, and public health as applicable.
<input type="checkbox"/> Cyberattack on Process Control Systems	
<input type="checkbox"/> Sabotage – Physical	
<input type="checkbox"/> Contamination of Source Water – Intentional	
<input type="checkbox"/> Contamination of Source Water – Accidental <sup>3</sup>	
<input type="checkbox"/> Other(s), enter below:	


<sup>3</sup> Accidental contamination is not a malevolent act. It is included here due to similar potential consequences and because whether a contamination incident is intentional or accidental may not be known during initial response.

Enter Community Water System Name


### Change History

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

Name/Title:	Date:	Description of Change:




Steps to prevent, detect, and  
eliminate hazards and threats in a  
small water system.





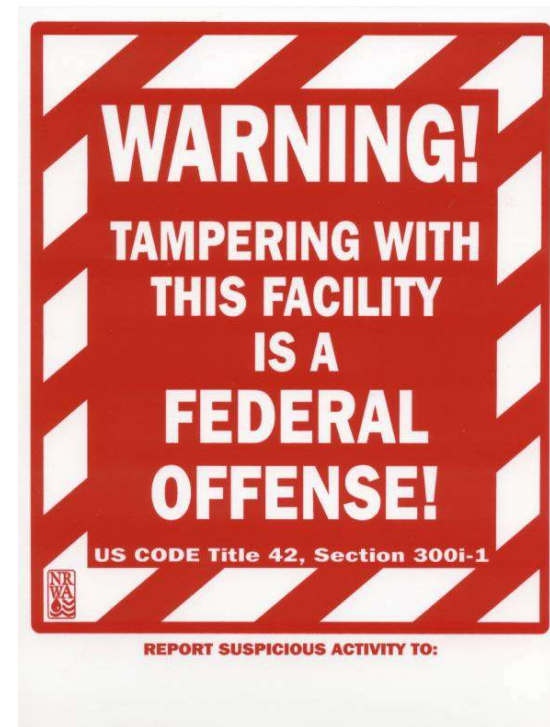


# Potential Risk Scenarios

- Unauthorized Entry into Utility Facilities
  - Water Contamination
  - Cyber Intrusion
  - Hazardous Chemical Release
  - Natural Hazards
  - Power Outages
- 

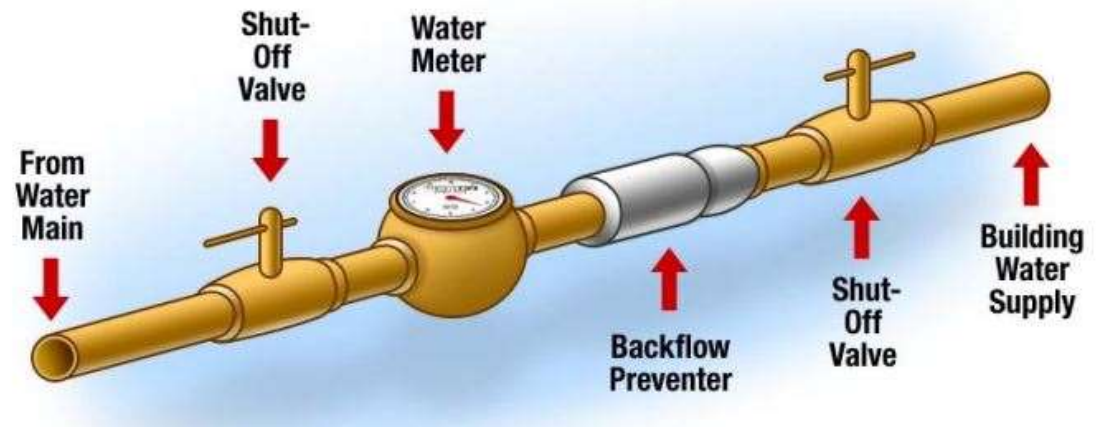
# Unauthorized Entry Into Utility Facilities

1. Communicate with Law Enforcement
2. Secure Facility
3. Limit Access
4. Post Signs



# Water Contamination

1. Test and Monitor Regularly
2. Inspect Infrastructure
3. Reduce Pollution
4. Educate the Public
5. Install Backflow Prevention
6. Tank Security
7. Hydrant Security



# Cyber Intrusion

1. Conduct Cyber Risk Assessment
2. Install Firewall/Antivirus
3. Train Staff
4. Strong Passwords(2 Step/Multifactor Authentication)
5. Backup Data
6. Stay in the Loop



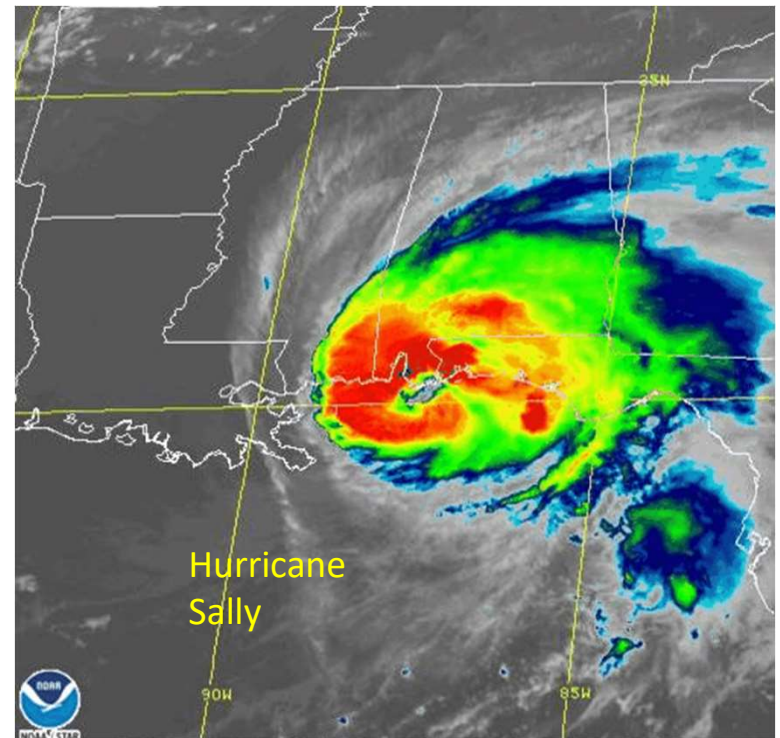
# Hazardous Chemical Release

1. Control and Track
2. Chemical Storage
3. Employee Training
4. Conduct Frequent Drills
5. Form Partnerships with Local  
Emergency Responders



# Natural Hazards

1. Identify Hazards
2. Assess Infrastructure Vulnerabilities.
3. Coordinate with Local Agencies and Utilities.
4. Exercises and Training
5. Post-Disaster



16 Sep 2020 08:35Z NESDIS/STAR GOES-East Band 13


# Power Outages

1. Install Auxiliary Power
2. Coordinate with Electric Utilities
3. Communicate with Public
4. Document Lessons Learned
5. Prioritize Facilities and Equipment





# Conclusion

- Analyze Whole System
  - Know Your Vulnerabilities
  - Prioritize Assets
  - Constantly Update Plan
  - Stay Aware
- 



**Be PROACTIVE!**

**THANKS!** 😊



**By: Tyler Grant**

ARWA WQAS, Operator Certification Trainer

***Email:*** [tgrant@alruralwater.com](mailto:tgrant@alruralwater.com)

***Phone:*** 334-451-7693