

Emergency Response Plans – What's the difference between PADEP's existing requirements and the federal AWIA requirements?

By Patti Kay Wisniewski, US EPA

The 2018 America's Water Infrastructure Act (AWIA) requires Emergency Response Plans (ERP) to include:

- Strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;
- Plans and procedures that can be implemented, and identification of equipment that can be utilized in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;
- Actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and
- Strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

Both EPA's and PADEP's requirements should be viewed as minimum aspects of ERPs. EPA Region 3 and PADEP's Bureau of Safe Drinking Water collaborated to conduct a review of these requirements to determine any differences between the two agencies' requirements. This article highlights the differences to assist community water suppliers with enhancing an existing ERP developed under the PADEP requirements such that it will comply with the AWIA requirements.

Pennsylvania's community water systems (CWS) should be aware that the AWIA requirements are **broader** than the current PADEP requirements. Below is a list of areas not included within the PADEP ERP template, **but are required by AWIA**:

- ERP distribution list and history of updates (highly recommended features)
- Detection Strategies (such as intrusion alarms, cyber threats, online water quality monitoring surveillance tools)
- Core Procedures which EPA describes as the "building blocks" for incident specific response procedures, since these apply across a broad variety of incidents:
 - Family well-being planning for responders and water employees
 - Access related challenges (e.g. road closures) and options to work around
 - Sampling and analysis plans
 - Incident Command System positions and roles, internally and with response partners
 - Physical security* (e.g. actions to be taken to secure a facility once an incident has occurred)

- Cyber security* (e.g. actions to be taken for added protection during an incident)

* While actions should be taken to harden facilities prior to any incident, additional actions may be necessary during an incident to further protect physical assets and connectivity. For physical security, this may include such things as added access control or lockdown procedures, and raising the level of attention to security during an incident. These are in addition to the day-to-day procedures.

As community water suppliers work to comply with AWIA's ERP requirements, please pay attention to these areas and ensure these are adequately covered in your plans. Nothing prohibits you from having plans that contain more information. Again, both EPA's and PADEP's requirements should be viewed as minimum aspects of ERPs. Your plans should be comprehensive to meet your specific needs and should be exercised on a regular basis and updated based on lessons learned from these exercises.

Patti Kay Wisniewski, US EPA, is the Drinking Water Preparedness and Resilience Coordinator