United States Environmental Protection Agency

GUARDING AGAINST TERRORIST AND SECURITY THREATS

Suggested Measures for Drinking Water and Wastewater Utilities (Water Utilities)

The Department of Homeland Security (DHS) established a five-tiered Homeland Security Advisory System to provide a national framework for notification about the nature and degree of terrorist threats. The system establishes a set of graduated levels that change in response to increases or decreases in terrorist threats. The threat levels are colored coded, beginning with green, and increasing in severity through blue, yellow, orange, and red. While the threat may not be specific to water utilities, the water sector, as one of the thirteen critical sectors identified by DHS, may consider themselves potential targets.

Why is EPA offering these suggestions?

Water utilities are in the forefront of ensuring that our nation's water systems are protected against terrorist threats. Many utilities have already developed safeguards. This document provides model guidelines for water utilities to increase security based on threat conditions described by the five-tiered Homeland Security Advisory System. Please note that the attached document is a guide; it is a not a requirement under any regulation or legislation.

This document provides suggested steps water utilities should consider implementing in the areas of detection, preparedness, prevention, and protection. The suggested measures are additive in that higher threat levels should also include those measures outlined in the document for lower threat levels. These suggestions are based on practices employed by various systems across the nation. The ability to implement them at the system level will vary. Note that these general recommendations should be adapted by the utility depending on the system size, status of emergency response planning at the utility, and identified system vulnerabilities. These suggestions should not be viewed as a complete source of information on protecting water utilities. Facility managers and utility security directors should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

Based on strong recommendations from the water sector, EPA is making this document available to water utilities and to the secure WaterISAC (www.waterisac.org). EPA is also providing this document to the state drinking water administrators. Some state homeland security and emergency response programs have issued suggestions to their critical infrastructures, including water. State drinking water administrators are encouraged to coordinate with state homeland security and emergency response programs and modify these suggested measures as appropriate to ensure consistency. **Please do not post this document on publicly available web sites.**

CONDITION	CONSIDER ADOPTING THESE MEASURES	
LOW (GREEN) **Low Risk of Terrorist Attack** signifies a **low risk** of terrorist attacks. Protective measures should focus on ongoing facility assessments; and the development, testing, and implementation of emergency plans. In addition to THREAT LEVEL GREEN, there are four higher threat levels: blue, yellow, orange, and red. (Please refer to the other fact sheets for information on suggested steps to be taken during other threat condition levels.)	Detection	▪ Monitor water quality at the source water, leaving the plant, and in distribution and storage systems. Establish baseline results. Review operational and analytical data to detect unusual variations. ▪ Follow-up on customer complaints concerning water quality and/or suspicious behavior on the facilities. ▪ Confirm communication protocol with public health officials concerning potential waterborne illnesses.
	Preparedness	▪ Post emergency evacuation plans in accessible, but secure, location near entrance for immediate access by law enforcement, fire response, and other first responders. ▪ Inventory spare parts and on-hand chemicals. Check if sufficient. ▪ Identify sensitive populations within the service area (e.g., hospitals, nursing homes, daycare centers, schools, etc.) for notification, as appropriate, in the event of a specific threat against the utility. ▪ Back-up critical files such as plans and drawings, as-builts, sampling results, billing, and other critical information. ▪ Conduct appropriate background investigations of staff, contractors, operators, and others with access to the facility. ▪ Prepare vulnerability assessments and revise to incorporate changes made (e.g., assets added/replaced or new countermeasures implemented). ▪ Ensure that employees understand appropriate emergency notification procedures.
	Prevention	▪ Train staff in safety procedures, such as handling hazardous materials and maintaining and using self-contained breathing apparatus. ▪ Secure equipment such as vehicles and spare parts. ▪ Monitor requests for potentially sensitive information.
	Protection	▪ Check all chemical deliveries for driver identification and verification of load. ▪ Maintain vigilance and be alert to suspicious activity. Inspect buildings in regular use for suspicious packages and evidence of unauthorized entry. Report any suspicious activity to appropriate authorities. ▪ Prosecute intruders, trespassers, and those detained for tampering to the fullest extent possible under applicable laws. ▪ Review request for tours and identify protocols for managing the tour. ▪ Implement controls for construction activities at critical sites. ▪ Maintain disinfectant residuals as required by regulations. ▪ Implement best management practices for optimizing drinking water treatment.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
GUARDED (BLUE) **General Risk of Terrorist Attacks** signifies a **guarded risk** of terrorist attacks. Protective measures should focus on activating employee and public information plans; exercising communication channels with response teams and local agencies; and reviewing and exercising emergency plans.	Detection	▪ Test security alarms and systems for reliability.
	Preparedness	▪ Reaffirm communication and coordination protocols (embedded in the utility's emergency response plan) with local authorities such as police and fire departments, HAZMAT teams, hospitals, and other first responders. ▪ Prepare and/or revise emergency response plans associated communication protocols. Include appropriate local officials concerned with law enforcement, emergency response and public health. ▪ On a regular basis post employee reminders about events that constitute security violations and ensure employees understand notification protocol in the event of a security breach. ▪ Prepare draft press releases, public notices and other communications for a variety of incidents. Route through appropriate channels of review to ensure pieces are clear and consistent.
	Prevention	▪ Secure buildings, rooms, and storage areas not in regular use. Maintain a list of secured areas or facilities and monitor activity in these areas.
	Protection	▪ Control access to mission critical facilities.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
ELEVATED **(YELLOW)** **Significant Risk of Terrorist Attack** signifies an **elevated risk** of terrorist attacks. Protective measures should focus on increasing surveillance of critical facilities; coordinating response plans with allied utilities and response teams and local agencies; and implementing emergency plans, as appropriate.	Detection	▪ To the extent possible, increase the frequency and extent of monitoring activities and review results against baseline. ▪ Increase review of operational and analytical data (including customer complaints) with an eye toward detecting unusual variability (as an indicator of unexpected changes in the product). Variations due to natural or routine operational variability should be considered first. ▪ Increase surveillance activities in source and finished water areas.
	Preparedness	▪ Review and update emergency response procedures and communication protocols**.** ▪ Establish unannounced security spot checks (e.g., verification of personal identification and door security) at access control points for critical facilities. ▪ Increase frequency for posting employee reminders of the threat situation and about events that constitute security violations. ▪ Ensure employees understand notification protocol in the event of a security breach. ▪ Conduct security audit of physical security assets, such as fencing and lights, and repair or replace missing/broken assets. Remove debris from along fence-lines that could be stacked to facilitate scaling. ▪ Maximize physical control of all equipment and vehicles inoperable when not in-use, (e.g., lock steering wheels, secure keys, chain and padlock on front-end loaders, etc.). ▪ Review draft communications on potential incidents, brief media relations personnel of potential for press contact and/or issuance of release. ▪ Review and update list of sensitive populations within the service area, such as hospitals, nursing homes, daycare centers, schools, etc., for notification, as appropriate, in the event of a specific threat against the utility. ▪ Contact neighboring water utilities to review coordinated response plans and mutual aid during emergencies. ▪ Review whether critical replacement parts are available and accessible.
	Prevention	▪ Carefully review all facility tour requests before approving. If allowed, implement security measures to include list of names prior to tour, request identification of each attendee prior to tour, prohibit backpacks/duffle bags, cameras and identify parking restrictions. ▪ On a daily basis, inspect the interior and exterior of buildings in regular use for suspicious activity or packages, signs of tampering, or indications of unauthorized entry. ▪ Implement mailroom security procedures. Follow guidance provided by the United States Postal Service.
	Protection	▪ Verify the identity of all personnel entering the water utility. Mandate visible use of identification badges. Randomly check identification badges and cards of those on the premises. ▪ At the discretion of the facility manager or security director, remove all vehicles and objects (e.g., trash containers) located near mission critical facility security perimeters and other sensitive areas. ▪ Verify the security of critical information systems (e.g., Supervisory Control and Data Acquisition (SCADA), Internet, email, etc.) and review safe computer and internet access procedures with employees to prevent cyber intrusion. ▪ Consider steps needed to control access to all areas under the jurisdiction of the water utility.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
HIGH (ORANGE) **High Risk of Terrost Attack** signifies a **high risk** of terrorist attacks. Protective measures should focus on limiting facility access to essential staff and contractors, and coordinating security efforts with local law enforcement officials and the armed forces, as appropriate.	Detection	▪ Increase the frequency and extent of monitoring activities. Review results against baseline. ▪ Confirm that county and state health officials are on high alert and will inform water utilities of any potential waterborne illnesses. ▪ If a neighborhood watch-type program is in place, notify the community and request increased awareness.
	Preparedness	▪ Confirm emergency response and laboratory analytical support network are ready for deployment 24 hours per day, 7 days a week. ▪ Reaffirm liaison with local police, intelligence, and security agencies to determine likelihood of an attack on the water utility personnel and facility and consider appropriate protective measures (e.g., road closing, extra surveillance, etc.). ▪ Practice communications protocol with local authorities and others cited in the facility's emergency response plan. ▪ Post frequent reminders for staff and contractors of the threat level, along with a reminder of what events constitute security violations. ▪ Ensure employees are fully aware of emergency response communication protocols and have access to contact information for relevant law enforcement, public health, environmental protection, and emergency response organizations. ▪ Inspect and practice activation of available emergency interconnections with neighboring water agencies. ▪ Have alternative water supply plan ready to implement (e.g., bottled water delivery).
	Prevention	▪ Discontinue tours and prohibit public access to all operational facilities. ▪ Consider requesting increased law enforcement surveillance, particularly of critical assets and otherwise unprotected areas.
	Protection	▪ Evaluate need to staff water treatment/production facility at all times. ▪ Consider the need to prohibit recreational use of surface water reservoirs. ▪ Increase security patrol activity to the maximum level sustainable and ensure tight security in the vicinity of mission critical facilities. Vary the timing of security patrols. ▪ Request employees change password on critical information management systems.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
SEVERE (RED) Severe Risk of Terrorist Attack signifies a **severe risk** of terrorist attacks. Protective measures should focus on the decision to close specific facilities and the redirection of staff resources to critical operations.	Detection	▪ Ensure that list of sensitive populations (e.g., hospitals, nursing homes, daycare centers, schools, etc.) within the service area is accurate and shared with appropriate public health officials. ▪ Reconfirm that county and state health officials are on high alert and will inform water utilities of any potential waterborne illnesses.
	Preparedness	▪ Post daily notices to staff regarding threat level and appropriate security practices ▪ Where appropriate, place back-up operational capacity on-line (water treatment plant filters, turbines, etc.). ▪ Ensure key utility personnel are on duty. ▪ Where appropriate, provide public notification for citizens to store emergency water supply or to implement other preparatory measures. ▪ Evaluate the need for opening an emergency operations center.
	Prevention	▪ As appropriate, request increased law enforcement and/or security agency surveillance, particularly of critical assets and otherwise unprotected areas (e.g., consider if National Guard assistance is needed and make appropriate request). ▪ Limit access to facilities and activities to essential personnel. ▪ Consider whether mail and packages should go to a central, secure location and be inspected before distribution. Remind mailroom personnel of the need for heightened awareness when sorting and distributing all incoming mail.
	Protection	▪ Ensure existing security policies, procedures, and equipment are effectively implemented. ▪ Recheck security of all on-site chemical storage and utilization areas. ▪ Implement frequent and staggered inspections of the exterior of buildings (to include roof areas) and parking areas. ▪ Re-check the security of critical information systems (e.g., SCADA, Internet, email, etc.) and have staff change computer passwords. ▪ Consider placing staff at remote (typically unmanned) facilities.