SECURITY MEASURES FOR WATER & WASTEWATER UTILITY FACILITIES

Critical infrastructure such as water and wastewater facilities may be targeted by criminals, vandals, saboteurs, and insiders. Physical barriers and security systems can be effective means to deter and prevent those who want to cause harm to utility facilities. The Guidelines for the Physical Security of Water Utilities (ANSI/ASCE/EWRI 56-10) and Guidelines for the Physical Security of Wastewater/Stormwater Utilities (ANSI/ASCE/EWRI 57-10) provide comprehensive recommendations for enhancing the physical security of water, wastewater, and stormwater utilities.

The guidelines classify potential threats into four Design Basis Threats (DBTs) categories, each with specific motives and capabilities yet all with the same goal of intending to interrupt the water treatment or delivery processes, contaminate the water, or trespass on the water utility property to commit a malevolent act:

1. **Vandal:** Targets property for defacement or damage without intent to harm individuals. Basic security measures typically suffice.
2. **Criminal:** Seeks valuable assets for theft and may use stealth or force. Requires more robust deterrence and delay strategies.
3. **Saboteur:** Motivated by political or ideological reasons, aiming to disrupt operations or cause public distrust. Needs advanced detection and delay measures.
4. **Insider:** Has authorized access but intends to sabotage or steal. Controlled through strict access management and background checks.

These guidelines emphasize a balanced approach to security through the integration of four primary elements:

1. **Deterrence:** Utilizing measures such as lighting, CCTV, and visible fencing to discourage potential adversaries.
2. **Detection:** Implementing sensors and surveillance systems to identify unauthorized access.
3. **Delay:** Installing physical barriers to slow down intruders until a response force can intervene.
4. **Response:** Ensuring proper actions are taken to interrupt adversary activities, involving utility staff, security personnel, or law enforcement as necessary.

To apply these guidelines effectively, utilities should undertake vulnerability assessments (VAs) using accepted methodologies like the Risk Assessment Methodology for Water (RAM-W) or the Vulnerability Self-Assessment Tool (VSAT). The resulting data informs the design and implementation of tailored physical security measures and technologies. The guidelines provide detailed recommendations on various security technologies and methods, including:

- Fencing and perimeter walls: The base level fence guideline is a galvanized steel chain-link fence with a post with a 6-foot or greater fabric height. The enhanced level fence guideline is a galvanized steel chain-link fence with a fence post with an 8-foot or greater fabric height.
- Gates and electronic access control systems.
- Intrusion detection sensors and CCTV systems.
- Barrier enhancements such as bollards and security lighting.

The New Jersey Office of Homeland Security offers this Facility Self Assessment Form and offers an on-site Vulnerability Assessment at no cost to your agency. If you are interested in inviting the NJ Office of Homeland Security to your facilities for an assessment, you can complete the Vulnerability Assessment Request Form.