To protect the public’s drinking water supply, law enforcement officials and local drinking water systems must work together to develop protocols for patrolling water systems and reporting and investigating any security breaches. A **credible threat** is an event that indicates potential contamination of a water supply. Trespassing, vandalism and thefts must be treated as credible threats until investigated and proven otherwise.

The following are **crimes** under the federal Safe Drinking Water Act.

- Tampering with a public water system; punishable by up to 20 years in prison and up to $1,000,000 fine.
- Attempting to tamper or threatening to tamper with a public water system; punishable by up to 10 years in prison and up to $100,000 fine.

**Tampering** is defined as introducing a contaminant into a public water system with the intention of harming persons, or interfering with the operations of a water system with the intent to harm.

So, how do you build an effective drinking water security program? Here are some tips.

- Be sure all personnel know the locations of water treatment plants, water tanks, raw water supplies, security perimeters and other vulnerable areas within the water treatment and supply system.
- Implement regular patrols of the areas mentioned above. Be sure all personnel are informed of any new infrastructure or changes in security systems and procedures.
- If there is a security breach, activate the water system’s emergency response or contingency plan, follow all local procedures and immediately alert:
  - the public water system;
  - local law enforcement office;
  - Ohio EPA, Division of Drinking and Ground Waters (district office); and
  - if terrorism is suspected, the FBI.
- Be aware of the penalties and fines assessed to anyone who tampers with a public water system.

Ohio EPA’s Division of Drinking and Ground Waters is pleased to foster relationships between public drinking water systems and Ohio’s law enforcement officials. When it comes to safe drinking water, we all have a stake in it.