Water Security Agency

EPB 363- Security at Water Treatment Plants

Delivering safe drinking water to your customers means ensuring there are appropriate security measures in place and knowing how to respond to an emergency. When you are prepared to respond to a crisis, the negative effects of the emergency can be minimized. Potential causes of emergencies include accidents (i.e. construction, traffic), backflow, fire/arson, hazardous material releases, terrorism and vandalism. Natural disasters that may cause an emergency include floods, forest and brush fires, severe cold weather/ice storms, tornadoes and waterborne disease outbreaks.

Monitoring various manmade (both intentional and accidental) threat information should be a regular part of a water treatment plant operator's job. As part of security planning, utilities should develop systems to access threat information, procedures that will be followed in the event of increased industry or facility threat levels and should be prepared to put these procedures in place immediately, so that adjustments are seamless. Involving local law enforcement and environmental project officers in your plan is critical.

Protect your customers from the negative outcomes which could include a shortage of drinking water, illnesses or deaths, public panic and fear of drinking the water from your system, long-term contamination of your water supply, costs of rehabilitating/rebuilding and/or decontaminating your water system, interruption of firefighting capability and interruption of sanitary services.

Detect, deter and minimize threats to reduce your system's vulnerabilities, improve the system's security and emergency response capability that protect public health. Because many water systems share common vulnerabilities, there are a number of solutions that most systems should consider. Although security improvements vary in complexity and cost, there are some relatively inexpensive, practical changes that can be implemented. Not all measures may be needed at your system - some may be more complex than what is needed for your community, others might address vulnerabilities that you've already remedied. Choose an action that deals with your system's highest priority security needs.

Daily Operational Activities: Facility signage should make it clear your utility is secure and monitored for intrusion. It should also indicate penalty for trespass is severe. Restrict facility access to authorized personnel. Establish employee identification including contractors and temporary workers with unescorted access to facilities.

- Check critical system components regularly.
- Know who has access to the facility and where the keys are. Record who has keys and stamp keys “Do Not Duplicate”. Change locks and access codes regularly.
- Require personnel to display photo ID at all times and wear uniforms or other identifying clothing. Require terminated or retired employees to return photo IDs, keys, access codes and uniforms.
- Increase the system security by denying access to unauthorized personnel. Supervised guests may be allowed. Verify IDs of employees who must access to water supply structures for maintenance and repair of equipment.
- Ensure all deliveries from vendors/suppliers are made in the presence of system personnel. Accept only deliveries scheduled in advance. Keep a delivery log. Require drivers to show vendor-issued ID. Verify that your suppliers take precautions to ensure their products are not contaminated.
- Identify all system vehicles prominently and require vehicles to be locked at all times. Remove critical information (ie. source water maps, plans) from vehicles before parking them overnight. Ensure fire/flood/ vandalism proof storage for these types of documents.
- Ensure safe storage of all hazardous materials for your plant. Store all chemicals in a secure, designated area. Keep an inventory of chemicals on hand and who has access to them.

Record Keeping: Define security-sensitive information; establish physical, electronic and procedural controls to restrict access to this information; detect unauthorized access; and ensure information and communications systems will function during emergency response and recovery.

- Store maps, records and other important documents in a secure location. Store backup copies of maps, records and other important documents in a secure, off-site location.
- Label all sensitive information "confidential" and require its return after projects are completed.
- Keep a record of employees who accessed sensitive information and the dates which they accessed it.
- If your system uses computers for operations or to store sensitive information, take steps to ensure information is protected and backed up. Back-up files, programs and computers regularly. Password-protect and virus-protect all computers. Change passwords and update virus protection programs regularly. By safeguarding your computers and paper records, you are delaying possible acts of sabotage.

Exterior: Know your water system and keep an eye on your facilities so you know when your security has been breached. Patrol your water system perimeter, check locks and other points of entry for signs of tampering and establish a neighbourhood watch program. Multiple security measures can slow down anyone who is trying to harm your system. Delaying an intruder gives you more time to detect a problem and more time to respond.

- Lock and consider alarming all points of entry: doors, windows, hatches, vents and gates. Install security fences around facilities. Lock all access points to finished water, even those within a locked or staffed building.
- Perform a visual examination of the exterior of your water treatment plant ensuring adequate exterior lighting around critical components. Remove objects that could be used to aid an intruder, such as ladders, overgrown shrubs and large rocks near windows and other points of entry.
- Do not park or allow vehicles to block the view of critical components. Clear fence lines of vegetation and overhanging branches. Install security fences around facilities.
- Once access to your system is restricted, back up restrictions to the facility by using security by patrol (periodically and randomly) and monitoring your facilities so you can detect any threats and intrusions.
- Consider these safety measures to keep intruders from your reservoir or well pump house - periodically, take a walk around your reservoir or well area to ensure no one has inadvertently left chemical containers or hazardous materials in the immediate area. Domestic water taken from a source that has a remote chance of becoming contaminated, should be fenced or, at a minimum, signage posted as a domestic municipal water supply. All pump houses should be locked at all times.
- When checking the security of underground reservoirs, make sure the entry hatches fit properly and are equipped with a solid hasp and a lock. Check the vents on underground reservoirs for proper screening.
- Water towers and elevated storage tanks need to be kept secure. All access hatches and doors should fit properly and should be safely locked. All vents are to be screened. Unauthorized access onto the tower should be prevented, for example by fencing off the tower or having a locked security cage on installed ladders.

In case of a security breach, contact your Environmental Project Officer (or if after hours, the 24-hour Water and Sewage Works Upset Reporting Line), your local law enforcement agency, your council or employer, and (if necessary) the fire department. An on-scene commander would notify the local Emergency Measures Organization.

Security Awareness – Part of Your Job!

An operator must always make physical security measures for all components of the water (and wastewater) utility a high priority each and every day and must include them in his daily operational routine. These measures must be included in Water Security Agency's Quality Assurance and Quality Control Policy for Waterworks EPB 542 that each facility must prepare. Also refer to Quality Assurance and Quality Control for Water Treatment Utilities EPB 243. Both publications are available on www.saskH20.ca/foroperators.asp under "Drinking Water Information Binder". Other websites list resources that an operator could access for more particular information on security include:

- Canadian Water and Wastewater Association (CWWA): www.cwwa.ca/publicationorder_e.asp (CWWA Vulnerability Assessment Template - CD-ROM)
- American Water Works Association: www.awwa.org/Communications/offer/secureresources.cfm
- USEPA - Water and Wastewater Security Product Guide: http://cfpub.epa.gov/safewater/watersecurity/guide/index.cfm
- Water Environment Federation: www.wef.org; enter "security" in the Search function.