Physical Security for Drinking Water Facilities

December, 2009

State of Oregon
Oregon Health Authority
Drinking Water Program

In Association with

The City of Gresham Water Utilities
The City of Portland Water Bureau
The Tualatin Valley Water District
And
The Regional Water Providers Consortium; Emergency Planning Committee

Best Practices for Physical Security
For public water systems in Oregon

As an outcome of the events of 9-11-2001, there has been an increased effort to protect critical infrastructures at the national, state and local levels. Since Drinking Water has been identified as one of these critical infrastructures it's no surprise that considerable attention is being focused on drinking water system security.

Historically, emergency response planning and security have been an integral part of water system operations, with the primary focus on natural disasters, system malfunctions and vandalism. Today, however, intentional acts of sabotage and terrorism must also be thrown into the mix. Whether the threat is international or domestic, water systems must begin to look at the security of their systems and incorporate scenarios and remedial actions into their emergency response planning to reflect these new concerns.

This guide is designed to provide the operator of drinking water facilities with a reference for evaluating their systems security posture, and references and resources to improve them.

The material contained in this form is based, in part, on the State of Oregon's *Model Emergency Response Plan*, the Association of State Drinking Water Administrators (ASDWA) and the National Rural Water Association's (NRWA) *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, and the American Society of Civil Engineers, American Waterworks Association & Water Environment Federation's *Guidelines for the Physical Security of Water Utilities.* For your reference, these tools can be downloaded at the Drinking Water Program's security website: http://www.oregon.gov/DHS/ph/dwp/security.shtml

Additionally, a visual dictionary of security equipment will be maintained at the above website, to allow the operators to familiarize themselves with the types and kinds of security equipment available for water systems. Suggestions and recommendations for content are always welcome.

Assessing the needs of the facility

Prior to developing a plan to improve a facilities physical security, the operator must conduct a vulnerability assessment. Without a vulnerability assessment, all of the efforts towards improving security will be haphazard at best. Additionally, the purpose of any security feature for water system protection is three fold; to *delay* the intruder, allowing you time to *detect* their presence, and then to *respond* to the intrusion, preferably by intercepting the threat prior to any access to treated or finished water can occur.

When conducting this vulnerability assessment, several key points need to be considered. First, what type of facility is it? A very small system with nothing more than a well, a pump, and a pressure tank will need significantly different protection than a large system consisting of multiple sources and treatment facilities, satellite locations like reservoirs, pump stations, and chemical storage facilities.

Second, what type of threat will the security be geared toward? Defeating the threat posed by an outside agent is usually much different than defeating the threat posed by an internal agent working against the system, but both should at least be considered.

Third, what are your known vulnerabilities? This can range from key components that the system cannot function without, to identifying equipment or facilities that may not be locked or secured at all.

Finally, the operator must decide the level of protection the system will be best served by. Generally, there are three levels of security for consideration, with increasing levels of protection for your clients. A low security facility might be the very small system above, where good quality locks and solid core steel access doors might be all that is needed to adequately protect the facility. Medium and high security facilities will generally have increasing layers of security, and be designed around multiple asset locations and settings.

Throughout the rest of this document, guidelines for the low, medium, and high security facilities will be explained, along with recommended layers for each. Determining which level of security is best for your assets, as well as an implementation schedule, will be the responsibility of the operator and is outside the scope of this document.

Finally, all of the above assumes the facility has an active, on-going review process for their vulnerability assessment process, an approved emergency response plan that is updated annually, and an up-to-date operations and maintenance manual. All of these documents are absolutely required to adequately protect the public we serve, and are also required by statute.

Low Security Facility

For low risk / low security systems, the minimum physical controls will generally include the following:

- Quality solid wood doors.
- Good quality locks on all access doors.
- “No Trespassing” and “Authorized Personnel Only” signage on entry doors and fencing.
- Standard 6’ security fencing around facility assets.
- Facility lighting to prevent hiding places.
- All critical control computer / SCADA systems separated from the internet via software & hardware firewall.

Additional security protocols *could* include:

- Routine patrols of facility assets by local law enforcement

- Key control program: How many keys do you have, who has them, and what to do when a key is lost or stolen? Additionally, marking keys such that each key can be tracked and accounted for could be a part of this process, to prevent unauthorized copies from being made.

- Employee turn-over / termination protocols: Key issuance and collection, password change requirements for computers / SCADA systems, uniform and other utility issued equipment collection when an employee leaves or is terminated.

Medium Security Facility

For medium risk / medium security systems, the minimum physical controls should include all items listed previously, and:

- Commercial steel security doors
- Commercial grade security locks on all access doors. Consider electronic locks and key access.
- Alarms on all exterior access doors, especially on those protecting finished water or critical components
- CCTV / video surveillance of critical equipment and associated entry points
- Enhanced fencing with barbed / concertina wire, and signage every 50 feet.
- Always on exterior lighting at perimeter, and motion activated lighting on interior buildings and storage facilities.
- Defensive landscaping to include removal of shrubbery / plants at least 25 feet from perimeter line, and is maintained such that it provides no cover or concealment for intruders.
- Bollards or Jersey barriers to control vehicle access to facilities or equipment.
- Employee ID (with picture) and uniform requirements.
- All critical control computer / SCADA systems separated from the internet via software & hardware firewall as a minimum, preferably by physically separating critical control equipment from the internet entirely.

Additional security protocols *should* include:

- Routine patrols of facility assets by local law enforcement

- Consider inviting law enforcement and other first responders to your facility to familiarize themselves with facility assets and layout.

- Key control program: How many keys do you have, who has them, and what to do when a key is lost or stolen? Additionally, marking keys such that each key can be tracked and accounted for should be a part of this process, to prevent unauthorized copies from being made. Alternatively, high security lock systems include special proprietary keys that can only be copied through the manufacturer, preventing unauthorized copies from being made.

- Background checks conducted on all employees

- Employee turn-over / termination protocols: Key issuance and collection, password change requirements for computers / SCADA systems, as well as uniform and other utility issued equipment collection when an employee leaves or is terminated.

High Security Facilities

For high risk / high security systems, the minimum physical controls will include all items listed previously, and:

- Commercial steel core security doors and high security frames / mounting hardware.
- Commercial grade security locks and dead bolts on all access doors, with access to controlled or restricted areas by photo ID key / card only via electronic locks.
- Alarms on all access doors and gates.
- CCTV / video surveillance of critical equipment and associated entry points, facility perimeters and approaches, as well as vehicle storage and parking. CCTV / video surveillance should also cover any area the public has access to, including business offices and public parking.
- Enhanced climb-proof fencing with barbed / concertina wire, foundation improvements to prevent tunneling, signage every 50 feet, and climb / cutting sensors.
- Always on exterior lighting at perimeter, motion activated lighting on interior buildings and storage facilities, tied into CCTV / video surveillance and alarm system.
- Defensive landscaping to include removal of shrubbery / plants at least 50 feet from perimeter line, earthen berms or barriers to control access, and is well maintained such that it provides no cover or concealment for intruders.
- Bollards or Jersey barriers to control vehicle access to facilities or equipment.
- Roving and fixed security on facility grounds.
- All critical control computer / SCADA systems separated from the internet by physically separating critical control equipment from the internet entirely.

Additional security protocols *must* include:

- Routine patrols of facility assets by local law enforcement

- Inviting law enforcement and other first responders to your facility to familiarize themselves with facility assets and layout, and making arrangements for them to utilize the facility for training purposes.

- Key control program: How many keys do you have, who has them, and what to do when a key is lost or stolen? Additionally, marking keys such that each key can be tracked and accounted for must be a part of this process, to prevent unauthorized copies from being made. Finally, high security lock systems include special proprietary keys that can only be copied by obtaining the necessary key blanks directly through the manufacturer, preventing unauthorized copies from being made.

- Background checks conducted on all employees

- Employee turn-over / termination protocols: Key issuance and collection, password change requirements for computers / SCADA systems, uniform and other utility issued equipment collection when an employee leaves or is terminated.

Item	Low Security	Medium Security	High Security
Perimeter			
Fencing	✓	✓	✓
No Trespassing signage every 50 feet	✓	✓	✓
Height greater than 6'		✓	✓
Barbed or concertina wire		✓	✓
tunneling resistant			✓
Climb / cut resistant		✓	✓
Climb / cut sensors			✓
Gates with locks and alarms	✓	✓	✓
Keycard access			✓
Manned gates			✓
Lighting - always on	✓	✓	✓
Lighting - motion sensor activated		✓	✓
Bollards or Jersey barriers to limit vehicle access		✓	✓
Clear sight zones around entire perimeter		✓	✓
No shrubbery or trees within 25 feet of fencing or structures		✓	✓
Inner facility			
Motion activated lighting		✓	✓
Commercial quality solid core wood or steel doors	✓	✓	✓
Commercial quality locks and hardware	✓	✓	✓
Roving guard patrols			✓
Alarms on all entry points to critical components or finished water		✓	✓
CCTV of critical equipment and associated entry points		✓	✓