

Security Revisited

By Doug Osburn, Training Specialist

By now most of you have completed your system's Emergency Response Plan (ERP) with the required Vulnerability Assessment (VA). So what happens next?

As I was going through my bundles of paperwork, I came across the checklist for a VA that the National Rural Water Association developed when all this started. I thought I might jog your memory and bring these items to light again. The document you developed is living, meaning it needs to be updated at least annually. The only way most of these items will ever be implemented is with the board or council establishing a line item in the budget to ensure funds are dedicated to increase the security level of your facility. Most utilities will not have the resources to implement everything all at once, but with planning and dedication, taking small steps each year will result in improved security at your facility.

NRWA Checklist

1. Do you have redundancy?
 - Back up power (generators).
 - Spare pumps.
 - Spare parts for repairing critical items.
 - Can you use natural gas and electricity?
2. Have you reviewed the U.S. EPA Baseline Threat Information Document?
3. Is access to the critical components of the water system (i.e. a part of the physical infrastructure of the system that is essential for water flow and/or water quality) restricted to authorized-personnel only?
4. Are all critical facilities, including well houses and pump pits fenced, gated and locked where appropriate?
5. Are all critical doors, windows, and other points of entry such as tank roof hatches and vents kept closed and locked?
6. Is there external lighting around all critical components of your water system?
7. Are warning signs (tampering, unauthorized access, etc.) posted on all critical components (well houses and storage tanks) of your water system?
8. Do you patrol and inspect all source intakes, buildings, storage tanks, equipment, and other critical components?
9. Is the area around all the critical components of

your water system free of objects that may be used for breaking and entering?

10. Are all the entry points of your water system easily seen?
11. Do you have an alarm system that will detect unauthorized entry or attempted entry at all critical components?
12. Do you have a key control and accountability policy?
13. Are entry codes and keys limited to water system personnel only?
14. Do you have an updated operations and maintenance manual that includes evaluations of security systems?
15. Do you have a neighborhood watch program for your water system?
16. Are your wellheads sealed properly?
17. Are well vents and caps screened and securely attached?
18. Are observation, test and abandoned wells properly secured to prevent tampering?
19. Is your surface water source secured with fences or gates? Do water system personnel visit the source?
20. Are deliveries of chemicals and other supplies made in the presence of water system personnel?
21. Have you discussed with your supplier(s) procedures to ensure the security of their products?
22. Are chemicals, particularly those that are potentially hazardous (i.e. chlorine gas) or flammable, properly stored in a secured area?
23. Do you monitor raw and treated water so that you can detect changes in water quality?
24. Are tank ladders, access hatches, and entry points secure?

ASSET: PHYSICAL PLANT

Perimeter

1. Perimeter physical barriers, such as a fence or wall.
2. Locking of perimeter gates.
3. Patrolling perimeter by guards or electronic monitoring.

Accessibility

1. Main road access, secondary roads.
2. Vegetation (trees and shrubs) permit concealed access to or near facility.
3. Drainage ditches provide concealed approach.
4. Night lighting on perimeter.
5. Surveillance tools (cameras, sensors, dogs) protecting perimeter.

Response Issues

1. Main road access, secondary roads

maintained during inclement weather.

Attacker's Perspective

1. Observation: how can surveillance and information be gathered from looking in?
2. Cover and concealment: where can we base an attack from and not be seen?
3. Obstacles: what will impede our approach, how long will it take to bypass?
4. Key Features: what must we control, and for how long?
5. Avenues of Approach: for our attack and for a response unit.
6. Time to get in; time to conduct our attack.
7. Concern with leaving any signs of tampering or method of attack.
8. Can preplanning information be gathered: camera/video driving by?
9. File footage from public records, web sites.

Entry / Access Control

1. Limiting access to employees or people having valid business at the facility.
2. Controlling access by a posted guard or through electronic means.
3. Locking of doors and windows.
4. Strength of doors, windows and locks.
5. Entry codes and locksets.
6. Control of visitors, photo identification, sign in and out, and facility escorts.
7. Facility tours.
8. Security of fill and vent pipes of chemical and fuel storage tanks.

Additional Measures

1. Badging system required to be prominently displayed.
2. Challenge procedures for lack of security ID present/enforced/rewarded.
3. Public provided tours, are cameras permitted?
4. Is facility manned 24 hours?
5. Designated personnel and procedures to routinely patrol (each shift) around the Perimeter.
6. Designated personnel and procedures to routinely patrol (each shift) within the Facility.

Attacker's Perspective

1. Effectiveness of entry/access control.
2. What technique can be used to gain entry: tour, job interview, tourist, professional interest.
3. Can preplanning information be gathered: camera on tour, driving by.

schedule one of our staff to assist you in this endeavor.

Now that I'm the Training Specialist, I don't get to see all my friends as often but I hope to see you at one of our conferences or training classes.

Until then, I'll see you down the road.

It is our hope that you take these tips and develop a strategy that will improve the security at your water system. If you need help, please call our office to