CHARACTERISTICS AND COMMON VULNERABILITIES INFRASTRUCTURE CATEGORY: COMMUNITY WASTEWATER TREATMENT FACILITIES

Protective Security Division
Department of Homeland Security

DRAFT - Version 1, January 15, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require understanding the common vulnerabilities of critical infrastructures, identifying site-specific vulnerabilities, understanding the types of terrorist activities that likely would be successful in exploiting those vulnerabilities, and taking preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to exploit them. This report characterizes and discusses common vulnerabilities of community wastewater treatment facilities.

CHARACTERISTICS OF COMMUNITY WASTEWATER TREATMENT FACILITIES

Water System Profile

Wastewater is water that has been used. It includes substances such as human waste, food scraps, oils, soaps, and chemicals. Wastewater is derived from residential, commercial, and industrial activities. In homes, wastewater is produced from sinks, showers, bathtubs, toilets, washing machines, and dishwashers. Commercial and industrial activities also produce wastewater that must be treated prior to release to the environment. In addition to home and business production, wastewater can also be generated by storm runoff (referred to as inflow) and interception of ground water (infiltration). Because of potentially harmful substances that wash off roads, parking lots, and rooftops, this water must also be treated.

Wastewater is treated in a wastewater treatment facility prior to release. In 2002, the nation's wastewater infrastructure consisted of approximately 16,000 publicly owned wastewater treatment plants; 100,000 major pumping stations; 600,000 miles of sanitary sewers; and another 200,000 miles of storm sewers. About 73% of the population was served by these 16,000 municipal treatment plants; the remainder was served by privately owned systems. A small number of large wastewater treatment plants (approximately 2,500) located in urban areas provided services to about 75% of the population. The combined value of the treatment and collection system was estimated at more than $2 trillion.

The volume of wastewater produced by a community ranges from about 50 to 250 gal per capita per day (gpcd), depending on sewer uses. A commonly used value for domestic wastewater flow

is 120 gpcd. This water contains about 0.24 lb of suspended solids and 0.2 lb of biochemical oxygen demand (BOD). BOD is a measure of the strength of a wastewater. It is the quantity of oxygen used by a mixed population of microorganisms in the aerobic oxidation of the organic matter in the water. Approximately 99% of municipal wastewater is water.

Common Characteristics

All wastewater treatment systems consist of two basic components: collector sewers and a treatment facility (Figure 1). The treatment facility is usually located adjacent to a stream, river, or lake to facilitate discharge of the treated water. The location is selected to have a low elevation to promote gravity flow to the facility. Solids from the treatment process are disposed to licensed landfills or applied to the land.

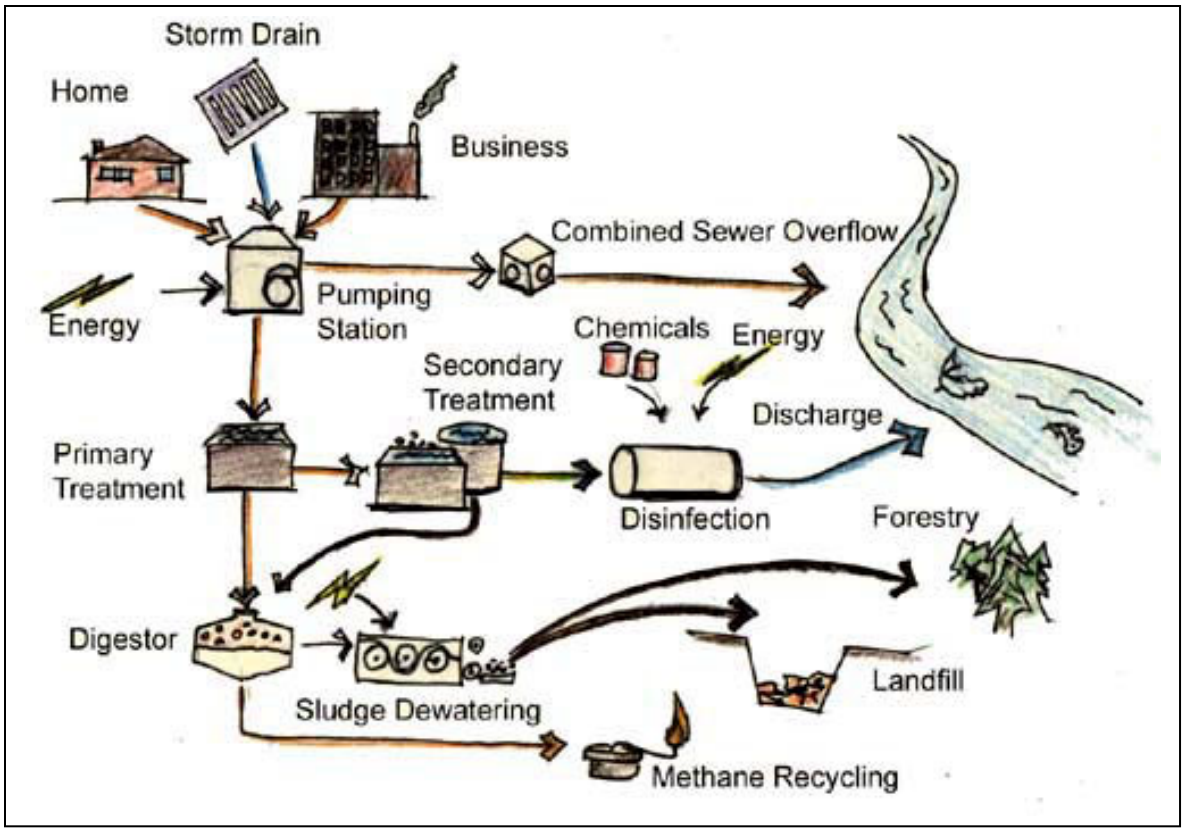

Figure 1 Generalized Schematic of a Wastewater Treatment Facility

Sewers are underground, watertight conduits that convey wastewater from its source to a treatment facility. Flow through the system can be driven by gravity, pumps, or both. A lateral sewer collects discharges from homes and carries them to another branch sewer. Branch or sub-main lines receive wastewater from the laterals and convey it to large mains. A main sewer line (trunk) carries the liquid from large areas to the treatment plant. If a pump drives the main line, it is referred to as a “force main.” Manholes are located at regular intervals to allow access to the pipes for inspection and cleaning. Lift stations are included in the collector system when

gravity flow is not possible. A pumping station can be installed to lift the wastewater to an intercepting sewer at a higher level, or it can discharge to a force main that conveys the wastewater to the treatment plant (Figure 2).

Figure 2 Lift Station in a Wastewater Collector System

Wastewater treatment is a combination of physical and biological processes that are designed to remove organic matter and other pollutants from solution. These processes include the following:

- Screening – Remove large objects (Figure 3)
- Grit removal – Remove sand, gravel, etc. (Figure 4)
- Flotation – Remove less-dense-than-water immiscible pollutants such as oil and grease

Figure 3 Wastewater Sewer Screen

- Flocculation and sedimentation (primary treatment) – Remove settable organic solids (e.g., Imhoff tanks – two-story septic tanks that separate an upper sedimentation zone from a lower sludge digestion chamber) (Figure 5)

Figure 4 Grinding Large Particles in Wastewater Prior to Removal

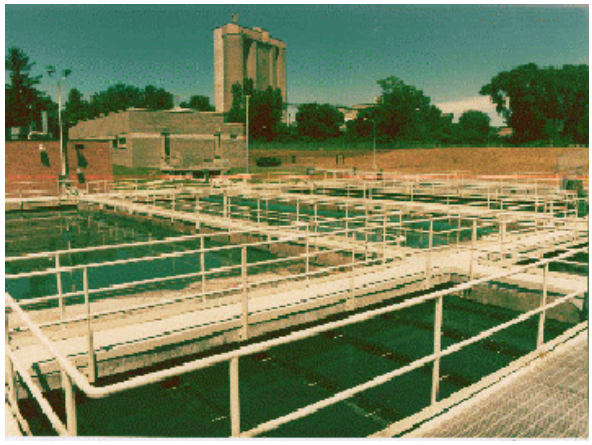

Figure 5 Primary Wastewater Treatment

- Suspended growth biological reactor/aeration – Remove dissolved organics (e.g., activated sludge method in which oxygen is bubbled through large tanks containing microorganisms and wastewater) (Figure 6)

Figure 6 Wastewater Aeration Basin

- Attached growth biological reactor – Remove dissolved organics (e.g., trickling filter method in which the wastewater is passed over a supporting structure, such as a bed of crushed rocks, that have attached microorganisms capable of eating the organic matter present)

- Clarification – Reduce turbidity of wastewater (Figure 7)

Figure 7 Wastewater Clarifier

- Disinfection – Reduce the number of pathogens (disease-carrying organisms) in the effluent (chlorination commonly used)

Figure 8 Chlorination Tank

- Chemical coagulation – Precipitate suspended solids, BOD, and phosphorous using lime, alum, iron salts, and polymers
- Nitrification – Convert ammonia to nitrate
- Denitrification – Reduce nitrate and nitrite to nitrogen gas
- Filtration – Remove suspended solids and reduce turbidity (Figure 9)
- Carbon adsorption – Remove soluble refractory organics
- Reverse osmosis – Demineralize the effluent (Figure 10)

Figure 9 Wastewater Filtration Unit

Figure 10 Small Reverse Osmosis Unit for Tertiary Treatment of Wastewater

The process of sedimentation is often referred to as primary wastewater treatment; the removal of large objects and grit is sometimes referred to as preliminary treatment. Biological treatment is referred to as secondary treatment. After primary and secondary treatment, about 85% of the pollutants in wastewater have been removed. Processes to remove the remaining pollutants, such as reverse osmosis, are referred to as tertiary or advanced treatment.

Depending on the application and characteristics of the wastewater, a typical wastewater treatment plant is a combination of the above processes. The processes are usually arranged in a "treatment train" (i.e., a series of processes applied in a sequence) to improve the quality of the wastewater to a degree at which it can be discharged to the environment. Discharge of the treated water is usually to a stream, river, or lake. The Environmental Protection Agency (EPA), under the National Pollutant Discharge Elimination System (NPDES) permitting program, regulates the degree of water purification needed prior to release.

Electric power is needed to operate municipal wastewater treatment systems. This electricity is used to operate pumps in the collector system and process the wastewater within the treatment facility.

In recent years, wastewater treatment systems have increased their reliance on supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs) for remote command and control of system components. Use of SCADA/DCS technologies allows tighter control of the treatment process, improved system efficiency, and decreased costs.

CONSEQUENCES OF EVENTS

Two main effects can be produced by attacks on wastewater treatment systems: denial of service, and hazardous chemical and biological releases. Although contaminants (e.g., Ricin) could be readily added to the wastewater stream at many locations in the collector system, such attacks would not produce significant impacts because of subsequent downstream treatment, large dilution by the receiving body of water, and lack of an immediate user. Denial is a disruption in the flow of wastewater from residences, businesses, and industries to and through a wastewater treatment facility. A denial of service can be accomplished by destroying trunk lines, collector pumps, lift stations, or equipment within the treatment facility itself. Without continued throughput of wastewater, contaminated water would remain in the system, or be pumped directly, if possible, to the receiving water without treatment. A buildup of pathogens would occur, which could lead to an outbreak of public diseases in the area of the collector system.

An attack on a wastewater treatment plant could also lead to the release of contaminated effluent to the receiving water of the plant. Such releases would primarily affect the environment; however, there could also be impacts to the general population if the receiving water is used as a water supply. Because wastewater treatment plants also use and store hazardous chemicals, an attack could discharge these contaminants to the environment, potentially impacting adjacent communities. For example, chlorine gas is a widely used disinfectant for secondary treatment of wastewater, which, if released into the environment, could have lethal effects.

From an attacker's point of view, a successful attack on a wastewater treatment system can produce two desirable effects. The first effect is to render the wastewater treatment process inoperable, thereby creating the potential for disease outbreak, environmental impacts, and a subsequent loss of revenue. The second effect is to create levels of fear that can result in societal disruption.

Wastewater treatment systems are vulnerable to three attack mechanisms: physical, electrical, and cyber penetration. Physical attacks could include destruction of trunk lines, collector pumps, lift stations, and mechanical components within the treatment facility. An attack on multiple targets could increase the effectiveness of the attack and lead to much longer down times for the facility. The direct impact of such attacks would be primarily environmental; however, with a pathogen buildup, disease outbreaks in the surrounding community are possible. Electrical attacks could be used to shut down key equipment, such as collector pumps, mixers, aerators, etc. With such equipment off-line, throughput could be severely restricted and environmental and health impacts could result. Similar to an electrical disruption, a cyber attack could be used to control key components of the collector system and the treatment facility. Impacts would be similar to those produced by an electrical disruption.

Community wastewater treatment systems are typically separate and independent of each other. These systems differ in the degree to which they require pumping, the kinds of filtration and treatment technologies employed, the nature of the water flow, and the composition of the water. These differences make causing a widespread impact to the overall treatment of wastewater extremely difficult, but attacking key systems can have a significant impact. Although the separate nature of systems may be an overall strength, it is also a vulnerability because there is

no direct way of getting wastewater from one system to another in the event of an emergency. In general, military installations do not have independent wastewater systems but rely on public systems. The following section provides information on the potential consequences of physical damage to or the destruction of the main wastewater system components.

Damage or Destruction

Physical damage to or the destruction of key components of the wastewater treatment system is considered to be the most likely threat against a wastewater treatment system. Such an attack could produce potentially large impacts to the community as well as to the environment.

Because of the large size of most wastewater collector systems, security is an issue. Access to trunk lines is readily available through regularly spaced manholes that are mostly unprotected. Similarly, lift stations and pumps are readily accessible to the terrorist.

Access to a wastewater treatment facility depends on its location. Because of the activities performed at wastewater treatment plants and the space required to perform some of the treatment processes (e.g., aeration), plants are often located away from large populations, thereby increasing their vulnerability to terrorists. If accessed, an attack on a wastewater treatment plant has the potential to disrupt service and release hazardous chemicals and biological materials to the environment. An attack on a wastewater treatment plant could also be designed to release hazardous chemicals (e.g., chlorine) stored at the facility. These chemicals are usually well-marked with hazard symbols, creating easily visible targets.

Many components of a wastewater treatment facility are located outside (i.e., not protected in a building). The exposure of components, such as pipes, storage containers, or even backup supplies, increases their vulnerability. Communication towers, such as radio-frequency and microwave towers, are also vulnerable. Physical damage to a treatment plant could potentially disrupt operations for several days to months, depending on the type and amount of damage done. Some large components in older systems were custom-made years ago and would be very difficult to replace if destroyed. As before, the duration of the supply disruption would depend on case-specific circumstances.

Increased reliance on SCADA and DCS technologies makes the wastewater treatment process more susceptible to cyber attack. Although most industry officials believe that firewalls provide adequate protection, a relatively proficient hacker with some basic knowledge about the wastewater treatment system could exploit this vulnerability.

STANDARDS

The American Water Works Association has published standards for pipe construction, installation, and performance. In addition, the EPA is responsible for regulating the quality of the treated water through its NPDES permitting program.

COMMON WASTEWATER TREATMENT SYSTEM VULNERABILITIES

Critical infrastructures and key assets vary in many characteristics and practices relevant to specifying vulnerabilities. There is no universal list of vulnerabilities that applies to all assets of a particular type within an infrastructure category. Instead, a list of common vulnerabilities has been prepared, based on experience and observation. These vulnerabilities should be interpreted as possible vulnerabilities and not as applying to each and every individual facility or asset.

The following is a list of common vulnerabilities found in wastewater treatment systems.

Exhibit 1 Economic and Institutional Vulnerabilities	
Economic and institutional vulnerabilities are those that would have extensive national, regional, and industry-wide consequences if exploited by a terrorist attack.	
1	Loss of wastewater treatment facilities could result in the contamination of drinking water supplies and create significant public health impacts.
2	Loss of wastewater treatment facilities could result in the restrictions on commercial and/or industrial activities. Without adequate facilities to handle their wastewater, these activities would need to be curtailed or would need to cease operation to avoid contaminating drinking water. There would be economic impacts from the restrictions on these activities.

Exhibit 2 Site-Related Vulnerabilities	
Site-related vulnerabilities are conditions or situations existing at a particular site or facility that could be exploited by a terrorist or terrorist group to do economic, physical, or bodily harm or to disable or disrupt facility operations or other critical infrastructures.	
Access and Access Control	
1	Public roads may be located near critical assets or entrance points.
2	Critical assets may be close to the perimeter fence.
3	Facilities may be located in remote, rural, or semi-rural locations with few or no facility personnel in the immediate area.
4	Public roads or rail lines pass over some critical assets.
5	Facilities may be unguarded and surveillance or other detection devices may be inadequate or not in use.
6	Delivery trucks may not be inspected.
7	Enclosure of critical facilities or assets may not be complete or adequate.
8	Signs to deter unauthorized personnel from entering facility grounds may not be posted.
9	Critical facilities and assets may be located on public land (e.g., river banks, shorelines, and public rights-of-way).

Exhibit 2 Site-Related Vulnerabilities	
Site-related vulnerabilities are conditions or situations existing at a particular site or facility that could be exploited by a terrorist or terrorist group to do economic, physical, or bodily harm or to disable or disrupt facility operations or other critical infrastructures.	
10	Gates and critical assets near the perimeter fence line may not be secured, controlled, or protected by barriers or other hardening equipment.
11	Security departments for municipally owned facilities may be understaffed.
12	Lighting may be inadequate (e.g., too little, poorly spaced, or improperly directed).
13	Entrances to critical assets within the facility (e.g., control rooms) may not have controlled access.
14	Access identification may not be required or may not be adequately enforced.
15	Employee and visitor parking may be located adjacent to critical buildings.
Operational Security	
16	Extensive background checks may not be conducted on employees and contractor personnel.
17	Coordination with local, state, and federal agencies on roles/responsibilities may be limited.
18	Web sites may provide detailed information on facility locations, critical assets, maps, and other operational data.
19	Critical assets may be marked with signage.
20	Hacking may provide adversaries with additional information.
21	Disgruntled employees may have knowledge of and access to vulnerable locations.
SCADA and Process Control	
22	Security may be lacking around servers and control rooms.
23	There is a potential for intruders to hack into SCADA process control through an enterprise network.
24	A controller could potentially cause an undesirable event.
25	A disgruntled employee could alter data or algorithms used to control the system.
Emergency Planning and Preparedness	
26	Contingency plans may not be formalized or exercised and may not include terrorism events.
27	Emergency operation center backup facilities may not be in place.
28	Spare parts that are large and/or expensive may be in short supply. Economic considerations may have reduced these spare part inventories. Some parts may have long manufacturing lead times.
	(*Continued on next page.)*

29	Facilities may be located in remote, rural, or semi-rural locations, leading to long response times for emergency and operational personnel.
30	Coordination of emergency plans with local, state, and federal government may be inadequate.
Hazardous and Toxic Chemicals	
31	Large quantities of chlorine or similar disinfectants may be stored on site for water purification and chemical processing.
32	Large storage tanks are easily identifiable from offsite.
33	Toxic chemicals may produce serious impacts, if released.
Other System Operation Considerations	
34	Damage to critical assets, plant processes, or pumping facilities could interfere with the utility's capability to effectively treat the wastewater.
35	The increased use of information management systems could cause potential vulnerabilities to the system through a cyber attack.

Exhibit 3 Interdependent Vulnerabilities

Interdependency is the relationship between two or more infrastructures by which the condition or functionality of each infrastructure is affected by the condition or functionality of the other(s). Interdependencies can be physical, geographic, logical, or information-based.

General	
1	Loss of chemical deliveries may reduce the ability to provide wastewater treatment.
2	Sewer rights-of-way are frequently identified with signs.
Natural Gas/Petroleum Products	
3	Many critical components (e.g., wells, pumps, and treatment facilities) that depend on electric power have backup emergency generators that burn natural gas or petroleum fuels.
4	Pipeline rights-of-way may be shared with natural gas pipelines or other utilities.
5	Restoration of service may require extinguishing a fire from a natural gas disruption.
Transportation	
6	Maintenance and repair of wastewater system components require the movement of personnel, equipment, and often heavy-duty vehicles (e.g., cranes) over distances that can be significant.
	(*Continued on next page.)*

7	Maintenance and repair of wastewater systems may require streets or roads to be torn up and then repaired.
8	Wastewater utilities rely on the transportation sector for access to remote facilities, delivery of treatment chemicals and other supplies, waste disposal, and other operational functions.
Electric Power	
9	Electric power may be needed to repair damages to wastewater systems.
10	Electric power is needed to operate wastewater system components, such as treatment facilities, pumps, etc., and to monitor and control operational conditions.
11	Sewer lines may be co-located with underground electric lines or on the same right-of-way as overhead lines.
12	Restoration of wastewater service may be of lower priority than restoring electric power. In some cases, repairs to the electric system must be done first to provide power to repair the wastewater system.
13	Wastewater utilities may lack sufficient backup generating power to meet their needs during an extended loss of electrical power.
Telecommunication	
14	Handheld radios may be critical in responding to wastewater system emergencies. Disruption of communications may delay notification of an incident and/or increase the response time.
15	Frequencies could be scanned by adversaries to determine operating conditions, location of employees, ongoing activities, etc.
16	Communication with first responders is crucial to react to incidents in a timely manner. Jamming or other methods may be used to disrupt communication channels.
17	Telecommunications rely on a public switching network. Telephone congestion occurs during emergencies.
18	Wastewater systems may rely on remote sensors to measure water flow, pressure, quality, and other operational parameters. Disrupting or altering the data from these remote sensors may result in the addition of incorrect chemicals, over-pressurization of the pipelines, or other disruptions, or it may cause an existing disruption to go undetected.
19	SCADA systems use the telecommunication network to communicate between sensors and control rooms, to provide information to maintenance and management personnel, and to provide data needed for accurate billing to customers.

In addition to the interdependencies listed above, officials must also consider that water is an unusual commodity in that it is continually used and reused. Water taken in by a water supplier may have been treated and discharged by another user farther upstream. This situation creates a unique interdependency among individual water and/or wastewater utilities. If the upstream dischargers are not sufficiently prepared for emergencies, they might release untreated or insufficiently treated water into a river that is the source for a downstream water supplier. Because the downstream water treatment facility is designed and operated on the basis of a certain water inlet quality, it may not be able to adequately treat the water entering the system during these situations. In such cases, the treated water might not meet applicable health standards.

OTHER INFORMATION

On June 12, 2002, President George Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) into law (P.L. 107-188). The Bioterrorism Act amends the Safe Drinking Water Act by adding Section 1433. Section 1433(a) requires that community water systems (CWSs) serving more than 3,300 users conduct security vulnerability assessments (SVAs), certify to EPA that the SVAs were conducted, and submit a copy of the SVAs to EPA. Section 1433(b) requires that certain CWSs prepare or revise their emergency response plans (ERPs) and certify that an ERP has been completed. The public water systems affected by Section 1433(b) represent only about 7% of the total number of public water systems in the United States (U.S.), but they provide service to 81% of all users.

For the past few years, the drinking water industry, in cooperation with EPA, has been working on projects to enhance security and protection. Many of these projects were under way prior to the attacks of September 11 and, subsequently, are already completed or near completion. Through these efforts, water utilities have already taken many straightforward, common sense actions to increase security and reduce threats from terrorism. Many of these actions are recommended by the American Water Works Association, the Association of Metropolitan Water Agencies, and other leading professional organizations. The recommendations include guarding against unplanned physical intrusion, making security a priority for employees, coordinating actions for effective emergency response, and investing in security and infrastructure improvements. EPA has also published manuals to assist water utilities in complying with requirements for increased security. For these manuals and other related material, refer to the EPA website (www.epa.gov/safewater/security).

In recent years, municipalities have tended to turn to the private sector to operate the community water supply systems. It is hoped that the private sector will be able to raise the capital needed for system expansion, maintenance, repair, and replacement for this rapidly growing and aging infrastructure. Financial considerations associated with increased security requirements also factor into this trend. In time, it will become more evident whether privatization leads to improved system operations and customer service, but it is currently too soon to make definitive statements in this regard.

The water infrastructure is one of the oldest infrastructures in the U.S. Many cities have major components in their water systems that are approximately 100 years old. Naturally occurring failures in these systems are increasing, with occasional large economic impacts. It is likely that these older components are more vulnerable to terrorist actions and that the consequences could be greater than for the same terrorist action taken against a newer system. In February 2001, EPA released the results of its 1999 Drinking Water Infrastructure Needs Survey, which led to the estimate that $150.9 billion is needed over the next 20 years to upgrade and repair water supply systems so as to ensure the continued provision of safe drinking water. Monetary requirements of this magnitude make it extremely difficult for water utilities to maintain existing systems, expand as needed to meet growing demands, and increase security, all at the same time. It is possible that the security enhancements are not receiving an appropriate share of the limited funding available to these utilities.

USEFUL REFERENCE MATERIAL

American Water Works Association (AWWA), *American Water Works Association Homepage*, accessed January 5, 2004 [http://www.awwa.org].

Analytical Services, Inc. (ANSER), *Journal of Homeland Security*, accessed January 6, 2004 [http://www.homelandsecurity.org/journal/articles.asp].

Association of Metropolitan Water Agencies (AMSA), *Clean Water on the Web*, accessed January 6, 2004 [http://www.amsa-cleanwater.org].

Association of Metropolitan Water Agencies (AMSA), *Asset Based Vulnerability Checklist for Wastewater Utilities*, accessed January 7, 2004 [http://www.amsa-cleanwater.org/pubs/2002avcheck.pdf].

Association of Metropolitan Water Agencies (AMSA), Clean Safe Water for the 21st Century, accessed January 5, 2004 [http://www.amsa-cleanwater.org/advocacy/winreport/winreport2000.pdf].

Association of State Drinking Water Administrators and the National Rural Water Association, *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, May 30, 2002.

Copeland, C., and B. Cody, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, accessed January 5, 2004 [http://www.ncseonline.org/nle/crsreports/03Jun/RS21026.pdf].

EPA, 1998, *How Wastewater Treatment Works: The Basics*, EPA 833-F-98-002, accessed January 5, 2004 [http://www.epa.gov/npdes/pubs/bastre.pdf].

EPA, *Alert on Chemical Accident Prevention and Site Security*, accessed August 11, 2003 [http://www.epa.gov/ceppo/pubs/secale.pdf].

EPA, *Counterterrorism Information*, accessed August 11, 2003 [http://www.epa.gov/ebtpages/ecounterterrorism.html].

EPA, *Drinking Water Security and Emergency Preparedness*, accessed January 5, 2004 [http://www.epa.gov/safewater/security/pdfs/fs_security_smallsuppliers_top10.pdf].

EPA, *Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, U.S. Environmental Protection Agency, Office of Water, accessed January 5, 2004 [www.epa.gov/safewater/security].

EPA, *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, accessed January 8, 2004 [http://www.epa.gov/safewater/security/security_act.pdf].

EPA, *Wastewater Technology Fact Sheet*, accessed January 8, 2004 [http://www.epa.gov/owmitnet/mtb/package_plant.pdf].

EPA, *What Wastewater Utilities Can Do Now to Guard Against Terrorist and Security Threats*, accessed January 6, 2004 [http://www.epa.gov/npdes/pubs/wastewaterutilityfactsheet.pdf].

EPA, *Municipalities and Wastewater Treatment Plants Factsheets and Outreach Materials*, accessed January 5, 2004 [http://cfpub2.epa.gov/npdes/docs.cfm?document_type_id=3&view=Factsheets%20and%20Outreach%20Materials&program_id=13&sort=name].

Ezell, Barry C., *Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply*, M.S. thesis, University of Virginia, May 1998, accessed July 27, 2000 [http://www.riskinfo.com/cyberisk/Watersupply/SCADA-thesis.html].

Grigg, Neil S., "Water Utility Security: Multiple Hazards and Multiple Barriers," *Journal of Infrastructure Systems*, June 2003.

Hammer, M.J. and M.J. Hammer, Jr., *Water and Wastewater Technology*, Prentice Hall: Englewood Cliffs, New Jersey, 1996.

Qasim, S.R., *Wastewater Treatment Plants Planning, Design, and Operation*, Holt, Rinehart, and Winston: New York, 1985.

Subcommittee on Water Resources and the Environment, *Terrorism: Are America's Water Resources and Environment at Risk*, accessed January 5, 2004 [http://www.house.gov/transportation/water/10-10-01/10-10-01memo.html].