POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: COMMUNITY WASTEWATER TREATMENT FACILITIES

Protective Security Division
Department of Homeland Security

Draft Version 1, January 30, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require identifying specific vulnerabilities at critical sites, understanding the types of terrorist activities—and the potential indicators of those 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 discusses potential indicators of terrorist activity with a focus on community wastewater treatment systems that collect wastewater from residences, businesses, and industries, and treats the wastewater prior to release to the environment.

INTRODUCTION

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack or that may be associated with terrorist surveillance, training, planning, preparation, or mobilization activities. The observation of any one indicator may not, by itself, suggest terrorist activity. Each observed anomaly or incident, however, should be carefully considered, along with all other relevant observations, to determine whether further investigation is warranted. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the community wastewater treatment facility of interest and what it might look like. The key factor in early recognition of terrorist activity is the ability to recognize anomalies in location, timing, and character of vehicles, equipment, people, and packages.

The geographic location and temporal proximity (or dispersion) of observed anomalies are important factors to consider. Terrorists have demonstrated the ability to finance, plan, and train for complex and sophisticated attacks over extended periods of time and at multiple locations distant from the proximity of their targets. Often, attacks are carried out nearly simultaneously against multiple targets.

Indicators are useful in discerning terrorist activity to the extent that they help identify:

- A specific asset that a terrorist group is targeting,

- The general or specific timing of a planned attack, and
- The weapons and deployment method planned by the terrorist.

In some cases, the choice of weaponry and deployment method may help to eliminate certain classes of assets from the potential target spectrum. Except for geographic factors, however, such information alone may contribute little to identifying the specific target or targets. The best indicator that a specific site or asset may be targeted is direct observation or evidence that the site or asset is or has been under surveillance. Careful attention to the surveillance indicators, especially by local law enforcement personnel and asset owners, is an important key to identifying potential terrorist threats to a specific site or asset. To increase the probability of detecting terrorist surveillance activities, employees, contractors, and local citizens need to be solicited to "observe and report" unusual activities, incidents, and behaviors highlighted in this report.

COMMUNITY WASTEWATER TREATMENT FACILITIES BACKGROUND

Terrorists Targeting Objectives

Community wastewater treatment facilities are attractive terrorist targets because of the impact that the loss of a treatment capability has on industrial and commercial enterprises, as well as on residential customers. As shown in Figure 1, terrorists or terrorist groups may target wastewater treatment facilities to either (1) sabotage the facility to halt or significantly decrease throughput, causing economic and potential health and environmental problems, or (2) release a hazardous material (e.g., chlorine) to the surrounding area, causing fear, illness, or death and burdening emergency services.

Sector Description

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, 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 prior to release in a wastewater treatment facility. 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 gallons 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.

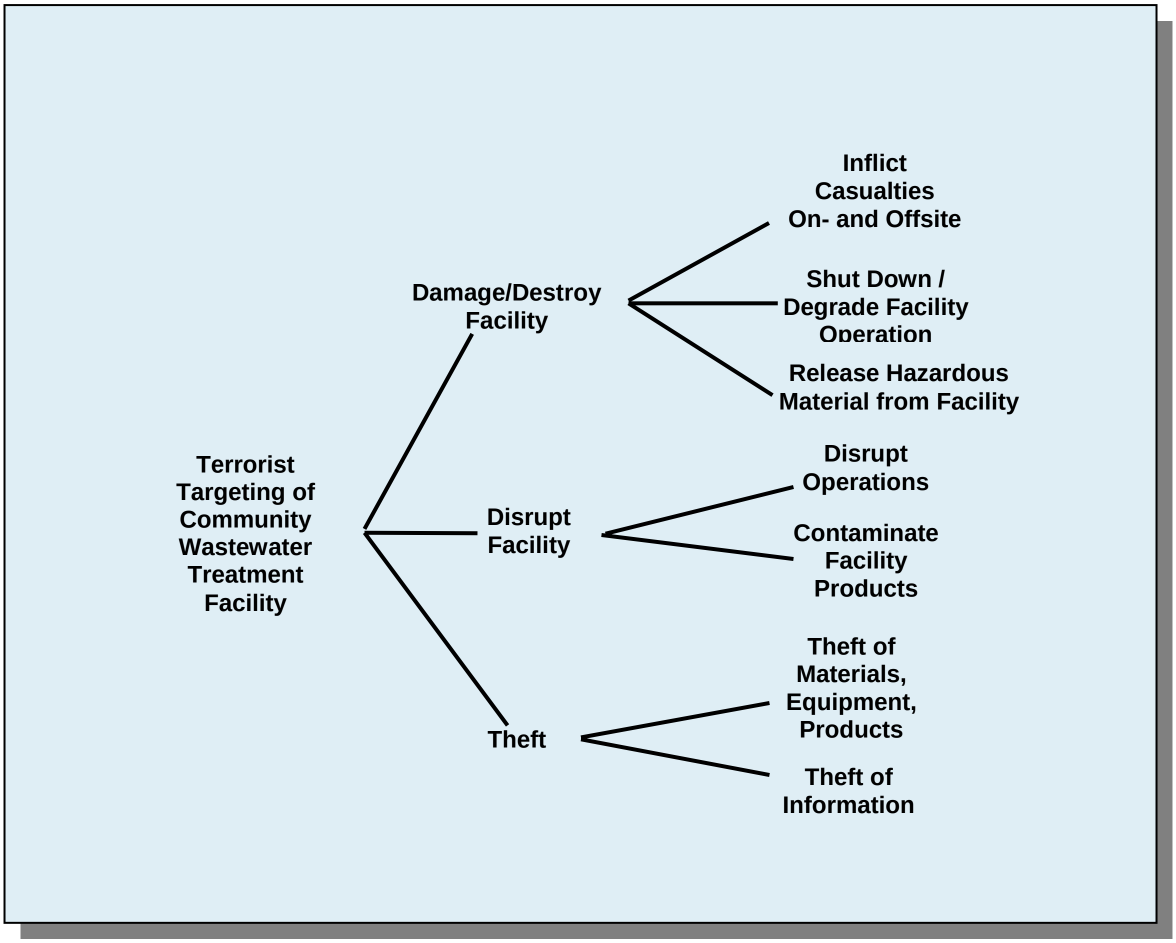
Terrorist Targeting of Community Wastewater Treatment Facility
Damage/Destroy Facility
Inflict Casualties On- and Offsite
Shut Down / Degrade Facility Operation
Release Hazardous Material from Facility
Disrupt Facility
Disrupt Operations
Contaminate Facility Products
Theft
Theft of Materials, Equipment, Products
Theft of Information

Figure 1 Terrorist Targeting Objectives for Wastewater Treatment Facilities

Common Characteristics

All wastewater treatment systems consist of two basic components: a treatment facility (Figure 2) and collector sewers. 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.

Sewers are underground, watertight conduits that convey wastewater from its source to a treatment facility. Flow through the system can be driven by gravity or pumps, or a combination of both. A lateral sewer collects discharges from homes and carries them to another branch sewer. Branch or submain 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 the main line is driven by a pump, 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 they can discharge to a force main that conveys the wastewater to the treatment plant.

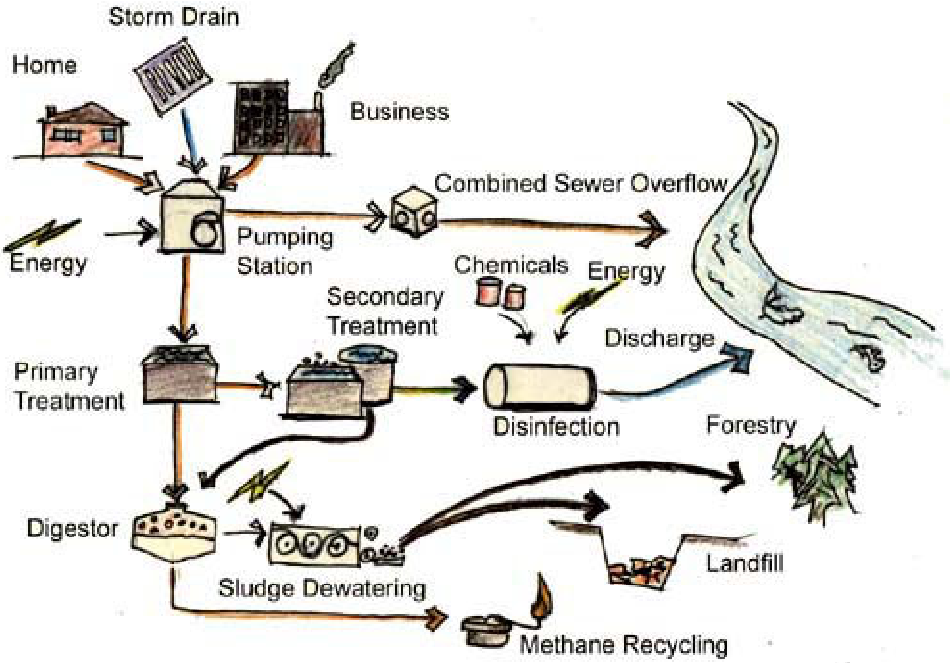

Figure 2 Generalized Schematic of a Wastewater Treatment Facility

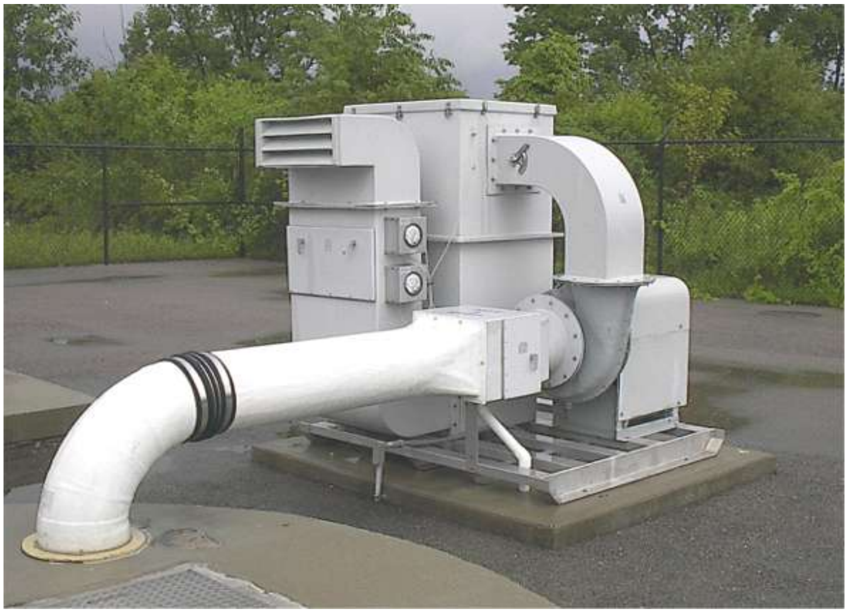

Figure 3 Lift Station in a Wastewater Collector System

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.

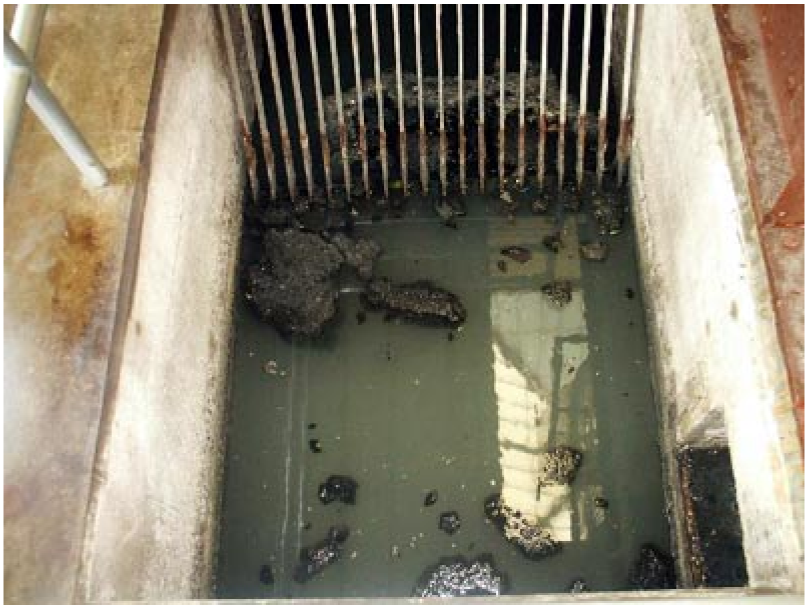

Figure 4 Wastewater Sewer Screen

- Grit removal – Remove sand, gravel, etc.

Figure 5 Grinding Large Particles in Wastewater Prior to Removal

- Flotation – Remove less-dense-than-water immiscible pollutants, such as oil and grease.
- Flocculation and sedimentation (primary treatment) – Remove settable organic solids (e.g., Imhoff tanks, which are two-story septic tanks that separate an upper sedimentation zone from a lower sludge digestion chamber).

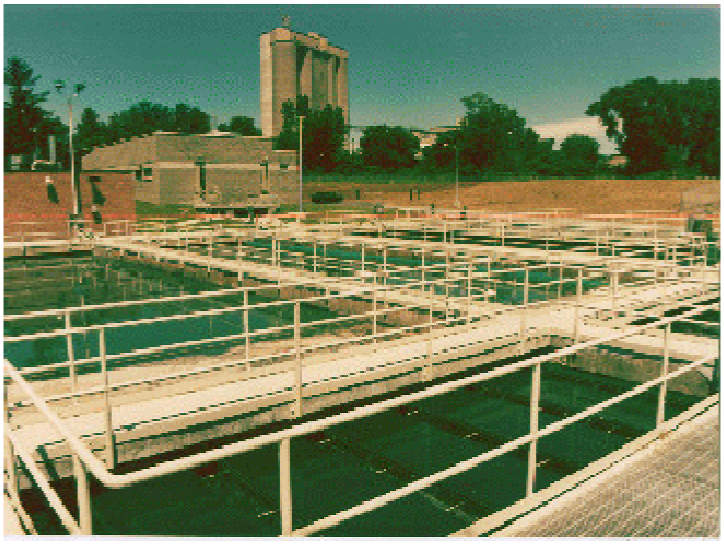

Figure 6 Primary Wastewater Treatment

- 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).

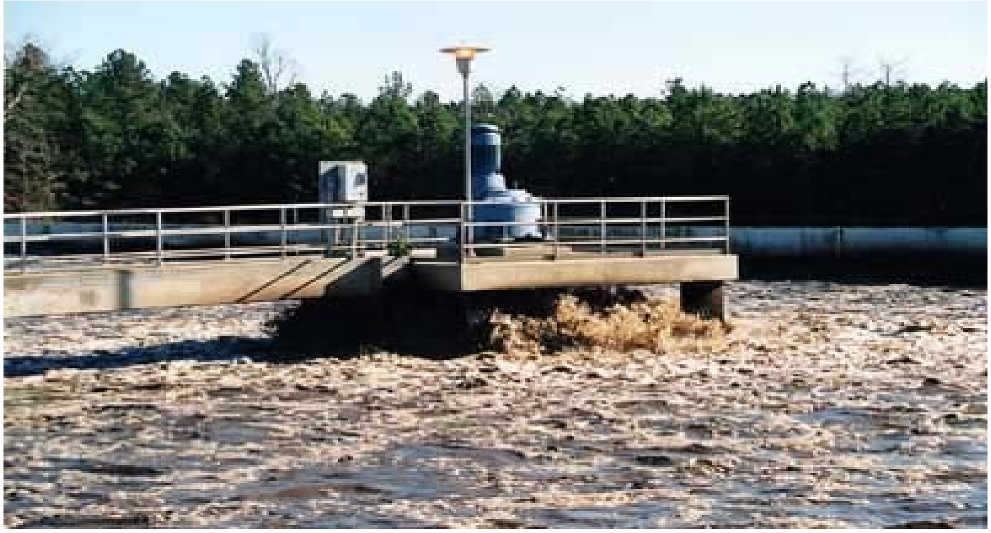

Figure 7 Wastewater Aeration Basin

- 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 microorganism capable of eating the organic matter present).

- Clarification – Reduce turbidity of wastewater.

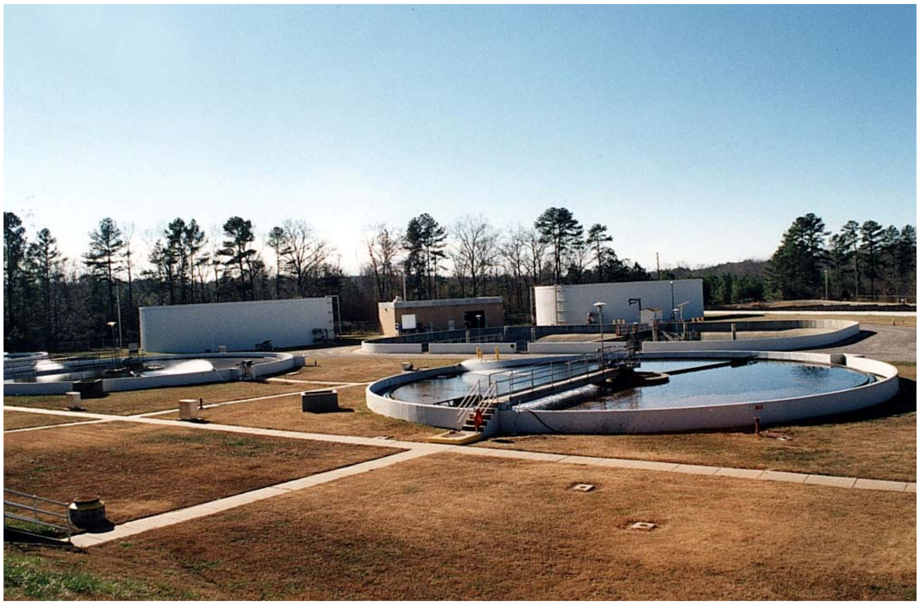

Figure 8 Wastewater Clarifier

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

Figure 9 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 10 Wastewater Filtration Unit

- Carbon adsorption – Remove soluble refractory organics.
- Reverse osmosis – Demineralize the effluent.

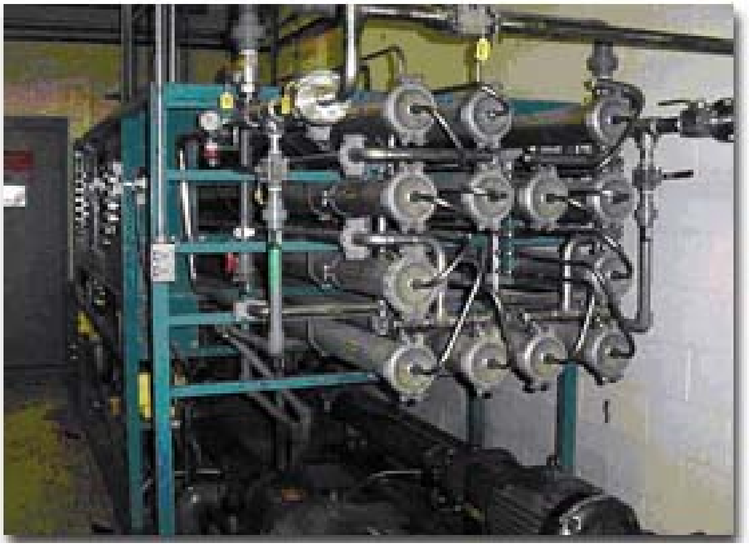

Figure 11 Small Reverse Osmosis Unit for Tertiary Wastewater Treatment

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 degree of water purification needed prior to release is regulated by the Environmental Protection Agency (EPA) under the National Pollutant Discharge Elimination System (NPDES) permitting program.

Electric power is needed to operate municipal wastewater treatment systems. Electricity is used to operate pumps in the collector system and to 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.

Damage or destruction of a wastewater treatment plant would result in untreated water being released into receiving bodies of water (e.g., rivers, lakes). To the extent that these bodies of water are used as drinking water supplies and/or as supplies of water for commercial or industrial activities, there could be serious public health and economic consequences from this disruption. Since many wastewater treatment plants have only a limited area to store untreated water, a disruption that resulted in the plant being out of services for several days could cause substantial impacts.

In addition to concerns about damage to a wastewater treatment facility, there is also a concern about the release of hazardous substances stored at these facilities. The Clean Air Act requires facilities with more than a threshold quantity of a listed extremely hazardous substance to have a risk management program in place and to submit a Risk Management Plan (RMP) to the EPA. The List of Regulated Substances includes 77 toxic substances and 63 flammable substances, which can be found in the *Code of Federal Regulations* (40 CFR 68). Chlorine, a common wastewater treatment chemical that is stored in large quantities at large wastewater treatment facilities, is an extremely hazardous substance. Information contained in an RMP for a facility of interest—including any water treatment facility using, storing, manufacturing, or handling chorine or any other toxic or flammable chemicals—can be helpful in understanding the specific facility assets that might be of interest to terrorist groups and the potential consequences of a successful attack.

Unfortunately, until 1999, RMP executive summaries were available publicly and could have been acquired by terrorist organizations. Currently, the executive summaries can no longer be accessed from the EPA website directly. The EPA keeps complete RMPs, including the offsite consequence analysis (OCA), which describes the demographics within a certain radius of the facility as well as environmental receptors within that radius. Other governmental agencies may have access to this information upon special request to the EPA. In addition, complete RMPs and OCA information are available (with certain restrictions) for viewing in paper form at EPA and Department of Justice (DOJ) Reading Rooms located throughout the U.S. Such access is required by Public Law 106-40 (the Chemical Safety Information, Site Security, and Fuels Regulatory Relief Act, Ref. 20). However, RMP information can be obtained for most covered facilities from the Right-to-Know Network [http://d1.rtk.net/rmp/wgrmp.php]. This website could be an important source of information for terrorists to use in selecting targets and estimating the consequences of their attack scenarios.

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored on a regular basis. Constant attention to these indicators can help to alert officials to the possibility of an incident.

Surveillance Indicators

Terrorist surveillance may be fixed or mobile. Fixed surveillance is done from a static, often concealed position, possibly an adjacent building, business, or other facility. In fixed surveillance scenarios, terrorists may establish themselves in a public location over an extended period of time or choose disguises or occupations such as street vendors, tourists, repair- or deliverymen, photographers, or even demonstrators to provide a plausible reason for being in the area.

Mobile surveillance usually entails observing and following persons or individual human targets, although it can be conducted against non-mobile facilities (i.e., driving by a site to observe the facility or site operations). To enhance mobile surveillance, many terrorists have become more adept at progressive surveillance.

Progressive surveillance is a technique whereby the terrorist observes a target for a short time from one position, withdraws for a time (possibly days or even weeks), and then resumes surveillance from another position. This activity continues until the terrorist develops target suitability and/or noticeable patterns in the operations or target's movements. This type of transient presence makes surveillance much more difficult to detect or predict.

More sophisticated surveillance is likely to be accomplished over a long period of time. This type of surveillance tends to evade detection and improve the quality of gathered information. Some terrorists perform surveillance of a target or target area over a period of months or even years. The use of public parks and other public gathering areas provides convenient venues for surveillance, because it is not unusual for individuals or small groups in these areas to loiter or engage in leisure activities that could serve to cover surveillance activities.

Terrorists are also known to use advanced technology such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices and global positioning systems. It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance, in this instance, refers to information gathering, legal and illegal, by terrorists using offsite computers. This type of data gathering might include obtaining site maps, key facility locations, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect data (e.g., damage or modify), software (e.g., damage or modify), or equipment/process controls (e.g., damage a piece of equipment or cause a dangerous chemical release by opening or closing a valve using offsite access to the SCADA system).

Terrorists may also use technical means to intercept radio or telephone (including cell phone) traffic.

An electronic attack could be an end in itself or could be launched simultaneously with a physical attack. Thus, it is worthwhile to be aware of what information is being collected from company and relevant government websites by offsite computer users and, if feasible, who is collecting this information. In addition, it is also important to know whether attempts are being made to gain access to protected company computer systems and whether any attempts have been successful.

The surveillance indicators in Exhibit 1 are examples of unusual activities that should be noted and considered as part of an assimilation process that takes into account the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other information at hand. For the most part, surveillance indicators refer to activities in the immediate vicinity of the community wastewater treatment facility; most of the other indicator categories in this report address activities in a much larger region around the facility.

Other Local and Regional Indicators

The remaining sets of indicators described in Exhibits 2–5 refer to activities not only in the immediate vicinity of the community wastewater treatment facility but also activities within a relatively large region around the facility (e.g., 100–200 miles). While local authorities should be aware of such activities, they may not be able to associate them with a specific critical asset because several may be within the region being monitored. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the wastewater facility of interest and what it might look like.

EXHIBITS

Every attempt has been made to be as comprehensive as possible in listing the following terrorist activity indicators. Some of the indicators listed may not be specific to the critical infrastructure or critical asset category that is the topic of this report. However, these general indicators are included as an aid and reminder to anyone who might observe any of these activities that they are indicators of potential terrorist activity.

Exhibit 1 Surveillance Indicators Observed Inside or Outside an Installation

What are surveillance indicators? Persons or unusual activities in the immediate vicinity of a critical infrastructure or key asset intending to gather information about the facility or its operations, shipments, or protective measures.

Persons Observed or Reported:

1	Persons using or carrying video/camera/observation equipment.
2	Persons with installation maps or facility photos or diagrams with facilities highlighted or notes regarding infrastructure or listing of installation personnel.
3	Persons possessing or observed using night-vision devices near the facility perimeter or in the local area.
4	Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
5	Non-military persons seen with military-style weapons and clothing/equipment.
6	Facility personnel being questioned offsite about practices pertaining to the facility, or an increase in personal e-mail, telephone, faxes, or mail concerning the facility or key asset.
7	Non-facility persons showing an increased general interest in the area surrounding the facility.
8	Facility personnel willfully associating with suspicious individuals.
9	Computer hackers attempting to access sites looking for personal information, maps, or other targeting examples.
10	An employee who changes working behavior or works more irregular hours.
11	Persons observed or reported to be observing facility receipts or deliveries, especially of hazardous materials.
12	Aircraft flyover in airspace over infrastructure facilities; boat encroachment into restricted areas, especially if near critical infrastructure.

(Continued on next page.)

Activities Observed or Reported:	
13	A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
14	Theft of facility or contractor identification cards or uniforms, or unauthorized persons in possession of facility ID cards or uniforms.
15	Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, security cameras, motion sensors, guard dogs, or other security devices.
16	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack planning activities.
17	Repeated attempts from the same location or country to access protected computer information systems.
18	Successful penetration and access of protected computer information systems, especially those containing information on site logistics, procedures, shipment schedules, security measures, passwords, and other sensitive information.
19	Attempts to obtain information about the facility (e.g., blueprints of buildings or information from public sources).
20	Unfamiliar cleaning crews or other contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas.
21	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
22	Increased interest in facility outside components (i.e., a lift substation not located on site and not as heavily protected or not protected at all).
23	Sudden increases in power outages. This could be done from an offsite location to test the backup systems or recovery times of primary systems.
24	Increase in buildings being left unsecured or doors being left unlocked that are normally locked at all times.
25	Arrest by local police of unknown persons. This would be more important if the facility or asset is located in a rural area rather than in or around a large city.
26	Traces of explosive or radioactive residue on facility vehicles during security checks by personnel using detection swipes or devices.
27	Increase in violation of security guard standard operating procedures for staffing key posts.
28	Increase in threats from unidentified sources by telephone, postal mail, or through the e-mail system.
29	Increase in reports of threats from outside known, reliable sources.
30	Sudden losses or theft of guard force communications equipment.
31	Displaced or misaligned manhole covers or other service access doors on or surrounding the facility or asset site.
32	Unusual maintenance activities (e.g., road repairs) near the facility or asset.
33	Observations of unauthorized facility or non-facility personnel collecting or searching through facility trash.

Exhibit 2 Transactional and Behavioral Indicators

What are transactional and behavioral indicators? Suspicious purchases of materials for improvised explosives or for the production of biological agents, toxins, chemical precursors, or chemicals that could be used in an act of terrorism or for purely criminal activity in the immediate vicinity or in the region surrounding a facility, critical infrastructure, or key asset.

Transactional Indicators:

What are transactional indicators? Unusual, atypical, or incomplete methods, procedures, or events associated with inquiry about or attempted purchase of equipment or materials that could be used to manufacture or assemble explosive, biological, chemical, or radioactive agents or devices that could be used to deliver or disperse such agents. Also included are inquiries and orders to purchase such equipment or materials and the subsequent theft or loss of the items from the same or a different supplier.

1	Approach from a previously unknown person (including those who require technical assistance) whose identity is not clear.
2	Transaction involving an intermediary agent and/or third party or consignee that is atypical in light of his/her usual business.
3	Approach from a person associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual request concerning the shipment or labeling of goods (e.g., offer to pick up shipment personally rather than arrange shipment and delivery).
5	Packaging and/or packaging components that are inconsistent with the shipping mode or stated destination.
6	Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
7	Unusual request for excessive confidentiality regarding discussions and/or transactions.
8	Orders for excessive quantities of personal protective gear or safety/security devices, especially by persons not identified as affiliated with an industrial plant.
9	Requests for normally unnecessary devices (e.g., an excessive quantity of spare parts) or a lack of orders for parts typically associated with the product being ordered, coupled with an unconvincing explanation for the omission of such an order or request.
10	Theft/loss/recovery of large amounts of cash by groups advocating violence against government/civilian sector targets (also applies to weapons of mass destruction).
11	Customer does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
	(Continued on next page.)

Customer/Vendor Behavioral Indicators:

What are customer/vendor behavioral indicators? Actions or inactions on the part of a customer or vendor for equipment or materials that appear to be inconsistent with normal behavioral patterns expected from legitimate commercial customers.

12	Reluctance to give sufficient explanation of the chemicals or other suspicious materials to be produced with the equipment and/or the purpose or use of those chemicals or materials.
13	Evasive responses.
14	Reluctance to explain sufficiently what waste streams are to be generated by the facility using the treatment plant.
15	Reluctance to provide clear answers to routine commercial or technical questions.
16	Reason for purchasing the equipment does not match the customer's usual business or technological level.
17	No request made or declines or refuses the assistance of a technical expert/training assistance when the assistance is generally standard for the installation or operation of the equipment.
18	Unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
19	Plant, equipment, or item is said to be for a use inconsistent with its design or normal intended use, and the customer continues these misstatements even after being corrected by the company/distributor.
20	Contract provided for the construction or revamping of a plant, but the complete scope of the work and/or final site of the plant under construction is not indicated.
21	Theft of material or equipment with no practical use outside of a legitimate business facility or industrial process.
22	Apparent lack of familiarity with nomenclature, chemical processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in purchasing chemicals.
23	Discontinuity of information provided, such as a phone number for a business, but the number is listed under a different name.
24	Unfamiliarity with the "business," such as predictable business cycles, etc.
25	Unreasonable market expectations.

Exhibit 3 Weapons Indicators

What are weapons indicators? Purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out the intended action. Items of interest include not only guns, automatic weapons, rifles, etc., but also ammunition and equipment, such as night-vision goggles and body armor and relevant training exercises and classes.

Activities Observed or Reported:

1	Theft or sales of large numbers of automatic or semi-automatic weapons.
2	Theft or sales of ammunition capable of being used in military weapons.
3	Reports of automatic weapons firing or unusual weapons firing.
4	Seizures of modified weapons or equipment used to modify weapons (silencers, etc.).
5	Theft, loss, or sales of large-caliber sniper weapons .50 cal or larger.
6	Theft, sales, or reported seizure of night-vision equipment in combination with other indicators.
7	Theft, sales, or reported seizure of body armor in combination with other indicators.
8	Paramilitary groups carrying out training scenarios and groups advocating violence.
9	People wearing clothing that is not consistent with the local weather (also applicable under all other indicator categories).

Exhibit 4 Explosive and Incendiary Indicators

What are explosive and incendiary indicators? Production, purchase, theft, testing, or storage of explosive or incendiary materials and devices that could be used by terrorists to help carry out the intended action. Also of interest are containers and locations where production could occur.

Persons Observed or Reported:

1	Persons stopped or arrested with unexplained lethal amounts of explosives.
2	Inappropriate inquiries regarding explosives or explosive construction by unidentified persons.
3	Treated or untreated chemical burns or missing hands and/or fingers.

Activities Observed or Reported:

4	Thefts or sales of large amounts of smokeless powder, blasting caps, or high-velocity explosives.
5	Large amounts of high-nitrate fertilizer sales to non-agricultural purchasers or abnormally large amounts to agricultural purchasers.[1]
6	Large thefts or sales of combinations of ingredients for explosives (e.g., fuel oil,

	nitrates) beyond normal.
7	Thefts or sales of containers (e.g., propane bottles) or vehicles (e.g., trucks, cargo vans) in combination with other indicators.
8	Reports of explosions, particularly in rural or wooded areas.
9	Traces of explosive residue on facility vehicles during security checks by personnel using explosive detection swipes or devices.
10	Seizures of improvised explosive devices or materials.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Theft of truck or van with minimum one-ton carrying capacity.
13	Modification of light-duty vehicle to accept a minimum one-ton load.
14	Rental of self-storage units and/or delivery of chemicals to such units.
15	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
16	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
17	Unattended packages, briefcases, or other containers.
18	Unexpected or unfamiliar delivery trucks or deliveries.
19	Vehicles containing unusual or suspicious parcels or materials.
20	Unattended vehicles on or off site in suspicious locations or at unusual times.

[1] The Fertilizer Institute developed a “Know Your Customer” program following the terrorist incident at Oklahoma City. The information is available from TFI at http://www.tfi.org/.

Exhibit 5 Chemical, Biological, and Radiological Indicators

What are chemical, biological, and radiological indicators? Activities related to production, purchase, theft, testing, or storage of dangerous chemicals and chemical agents, biological species, and hazardous radioactive materials.

Equipment Configuration Indicators:

1	Equipment to be installed in an area under strict security control, such as an area close to the facility or an area to which access is severely restricted.
2	Equipment to be installed in an area that is unusual and out of character with the proper use of the equipment.
3	Modification of a plant, equipment, or item in an existing or planned facility that changes production capability significantly and could make the facility more suitable for the manufacture of chemical weapons or chemical weapon precursors. (This also applies to biological agents and weapons.)
4	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
5	Unattended packages, briefcases, or other containers.
6	Unexpected or unfamiliar delivery trucks or deliveries.
7	Vehicles containing unusual or suspicious parcels or materials.
8	Theft, sale, or reported seizure of sophisticated personal protective equipment, such as “A’” level Tyvek, self-contained breathing apparatus (SCBA), etc.
9	Theft or sale of sophisticated filtering, air-scrubbing, or containment equipment

Chemical Agent Indicators:

10	Inappropriate inquiries regarding local chemical sales/storage/transportation points.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Rental of self-storage units and/or delivery of chemicals to such units.
13	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
14	Treated or untreated chemical burns or missing hands and/or fingers.
15	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems.
16	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.

(Continued on next page.)

USEFUL REFERENCE MATERIAL

1. White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* Feb. 2003 [http://www.whitehouse.gov/pcipb/physical.html].

2. *Terrorist Attack Indicators* Html file: [http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators]; PDF file: [http://216.239.53.100/search?q=cache:YMHxMOEIgOcJ:afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%2520Pubs/Terrorist%2520Attack%2520Indicators.PDF+terrorist+attack+indicators&hl=en&ie=UTF-8].

3. U.S. Department of Homeland Security, "Potential Indicators of Threats Involving Vehicle-Borne Improvised Explosive Devices (VBIEDs)," *Homeland Security Information Bulletin,* May 15, 2003 [http://www.apta.com/services/security/potential_indicators.cfm]. This document includes a table of chemicals and other demolitions paraphernalia used in recent truck bomb attacks against U.S. facilities.

4. Defense Intelligence College, Counterterrorism Analysis Course, *Introduction to Terrorism Intelligence Analysis, Part 2: Pre-Incident Indicators* [http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm].

5. Princeton University, Department of Public Safety, *What is a Heightened Security State of Alert?* [http://web.princeton.edu/sites/publicsafety/].

6. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents* [http://www.kentuckystatepolice.org/terror.htm]. This site lists several indicators, protective measures, and emergency procedures.

7. U.S. Air Force, Office of Special Investigations, *Eagle Eyes: Categories of Suspicious Activities* [http://www.dtic.mil/afosi/eagle/suspicious_behavior.html]. This site has brief descriptions of activities, such as surveillance, elicitation, tests of security, acquiring supplies, suspicious persons out of place, dry run, and deploying assets.

8. Baybutt, Paul, and Varick Ready, "Protecting Process Plants: Preventing Terrorism Attacks and Sabotage," *Homeland Defense Journal*, Vol. 2, Issue 3, pp. 1–5, Feb. 12, 2003 [http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf].

9. U.S. Environmental Protection Agency, *Envirofacts Data Warehouse* [http://www.epa.gov/enviro/]. This site has information about EPA-regulated chemical facilities. For example, users can obtain maps showing the facility and lists of toxic chemicals used or produced at the site.

10. Risk management plans and executive summaries formerly available from the U.S. Environmental Protection Agency are currently available from the Right-to-Know

Network [http://d1.rtk.net/rmp/wgrmp.php]. This site has information listed by state for all chemical plants that have filed risk management plans. The executive summary includes a description of the worst-case release scenario for regulated toxic chemicals and regulated flammable chemicals.

11. 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.

12. EPA, *Drinking Water Security and Emergency Preparedness*.

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

14. Hammer, M.J., and M.J. Hammer, Jr., *Water and Wastewater Technology,* Prentice Hall, Englewood Cliffs, NJ, 1996.

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

RELATED WEBSITES

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

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

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

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

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

6. 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.

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

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

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

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

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

12. 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 [www.epa.gov/safewater/security], accessed Jan. 5, 2004.

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

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

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

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

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

18. Federal Bureau of Investigation (FBI) [http://www.fbi.gov], accessed Jan. 12, 2004.

19. Subcommittee on Water Resources and the Environment, *Terrorism: Are America's Water Resources and Environment at Risk*?

[http://www.house.gov/transportation/water/10-10-01/10-10-01memo.html], accessed Jan. 5, 2004.

20. The Right to Know Network [http://d1.rtk.net], accessed Jan. 12, 2004.

21. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp], accessed Jan. 12, 2004.