POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: FOSSIL-FUEL POWER STATIONS

Protective Security Division
Department of Homeland Security

Draft – Version 1, March 5, 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 fossil-fuel power stations.

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 fossil-fuel power station 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.

FOSSIL-FUEL POWER STATION BACKGROUND

Terrorists Targeting Objectives

Figure 1 depicts the range of possible objectives for a terrorist attack on fossil-fuel power stations. Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many terrorist acts. Casualties can occur both at the facility and in the surrounding area. Damage or destruction of the facility can be intended to shut down or degrade the operation of the facility, or to cause the release of hazardous materials to the surrounding area. Disruption of the facility without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. Theft of equipment, materials, or products can be intended to divert these items to other uses or reap financial gain from their resale. Theft of information can be intended to acquire insight that is not made public or gain data that can be used in carrying out attacks.

Specific threats that are of concern to fossil-fuel power stations include:

- Explosives (e.g., car bomb, suicide bomber),
- Stand-off weapons (e.g., rocket-propelled grenades),
- Interference with electrical equipment (e.g., short circuiting material), and
- Malicious control of equipment (e.g., through SCADA systems).

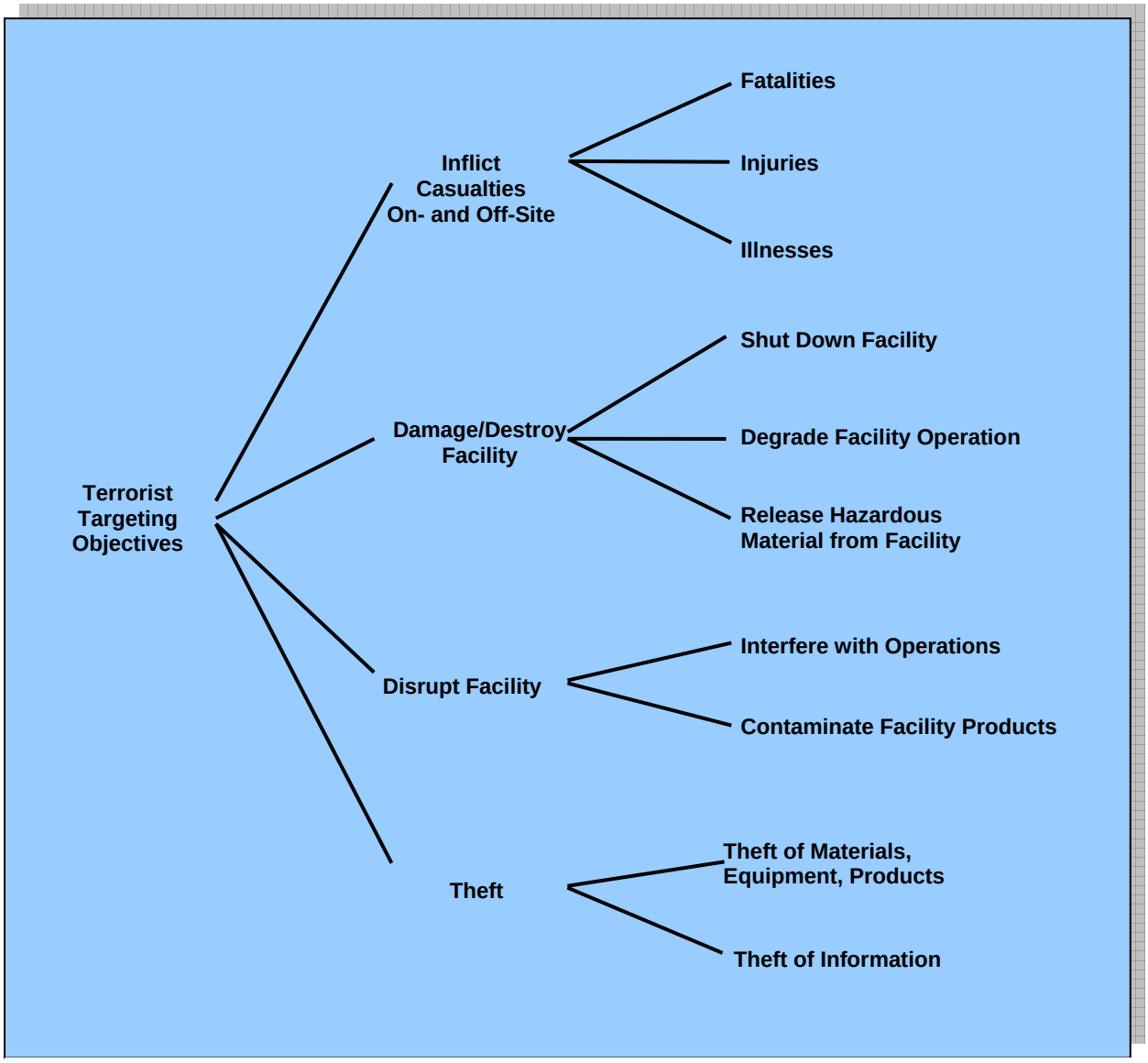

Figure 1 Potential Terrorist Targeting Objectives

Characterization of the Industry

Fossil-fuel power plants use coal, oil, and natural gas to generate electricity. In all fossil-fuel plants, the fuel is combusted and the resulting heat energy is used to produce electricity. In the United States (U.S.) in 2001, fossil-fuel generation accounted for about 70% of total electricity generation. The breakdown by fuel type was as follows:

- Coal 51%
- Natural gas 16%
- Oil 3%

Common Facility Characteristics

Four main types of power plants use fossil fuels: steam turbine, combustion turbine, combined-cycle (CC), and internal combustion engine.

Steam Turbine Power Plant

Steam power plants burn fossil fuel in the furnace of a steam boiler. Steam from the boiler expands through a steam turbine, which is connected to a drive shaft of an electric generator. The exhaust vapor expelled from the turbine condenses, and the liquid is pumped back to the boiler to repeat the cycle. Steam power plants are designed to use coal, natural gas, or oil. Before combustion gases can be exhausted to the atmosphere, they typically must be cleaned to reduce particulates, NO_x, and SO_2 to levels required by federal and state regulations.

Steam power plants are typically large units that range in size from about 50 to 1,200 megawatts (MW). Because these plants are large and designed for high reliability and efficiency, they are operated as long as possible and as closely to design capacity as possible. The operation of plants in this manner is termed “base loading” a plant; that is, the plant serves the portion of the electrical demand that is relatively constant throughout the entire day. The capacity factor (the ratio of the number of hours the plant operates in a year to the total number of hours in a year) of base-loaded plants often exceeds 65%.

Figure 2 shows a modern, coal-fired steam power plant. A conveyor to carry coal to the plant is shown on the left, and the cooling towers of the plant are shown on the right.

Figure 2 Modern Coal-Fired Steam Power Plant

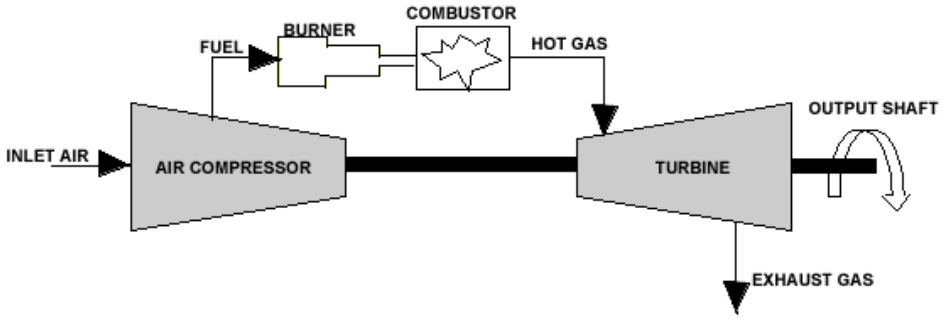

Figure 3 Schematic Diagram of a Combustion Turbine Generator

Combustion Turbine Power Plant

Combustion turbine plants burn gaseous or liquid fossil fuels, namely natural gas or various grades of oil. Combustion turbines are similar to aircraft jet engines. The fuel is burned in a combustor, and hot gases expand through a turbine, which drives a generator to produce electricity. Depending on the fuel and the regulatory requirements, exhaust gases may need to be cleaned before being released to the atmosphere. A schematic diagram of a combustion turbine generator is shown in Figure 3.

Combustion turbines used by electric utilities range in size from about 25 MW to about 250 MW. They are inexpensive, can be built quickly, and can be started and loaded very rapidly (as short as two minutes from start to full load). Because of these characteristics, they operate as peaking plants; that is, they operate only when necessary to satisfy the peak electrical demands of the day—generally only a few hours each day. Their capacity factors are typically no more than 10% to 15%. Because of their low capital cost, their operational flexibility, and the reasonable natural gas prices, combustion turbines, either stand-alone or in combined-cycle plants described in the following section, are expected to account for much of the new capacity to be installed in the near future by electric companies.

Combined-Cycle Power Plant

Combined-cycle power plants combine a combustion turbine with a steam boiler to produce electricity at a higher overall efficiency. The fuel, typically natural gas, is burned by using a combustion turbine, and hot gases expand through a turbine to produce electricity. The exhaust of the combustion turbine is then sent through a boiler, where steam is produced to drive a turbine/generator. This design substantially improves the overall efficiency of the combustion turbine or a conventional steam turbine. Figure 4 shows a schematic of one CC plant configuration.

Combined-cycle power plants used by electric companies can range in size from about 50 MW to almost 1,000 MW. Flexibility in size, coupled with operational flexibility, allows them to operate as either base- or intermediate-load plants. A plant operating in intermediate duty generates power to serve that portion of the load that is greater than the constant base load of the

electric system but less than the system peak loads. Capacity factors for intermediate-duty plants are in the 30% to 45% range.

Other advantages of CC power plants are a small plant footprint, minimal water consumption, a short construction schedule (two to three years from planning to commercial operation versus five or more years for a coal-fired station), and modular design, meaning that units of capacity can be easily added to the station as the system load grows. Figure 5 presents an artist's rendering of the modular CC design. Because of these advantages and the competitive prices of natural gas, U.S. electric companies have been constructing CCs (along with combustion turbines) to serve electrical demand in the near future.

CC plants can also be used to retrofit existing oil- and gas-fired steam units and to repower existing oil- and gas-fired combustion and steam turbines. Depending on the plant design and state and federal environmental regulations, CC power plants may need to install pollution controls to reduce NO_x and SO_2 emissions.

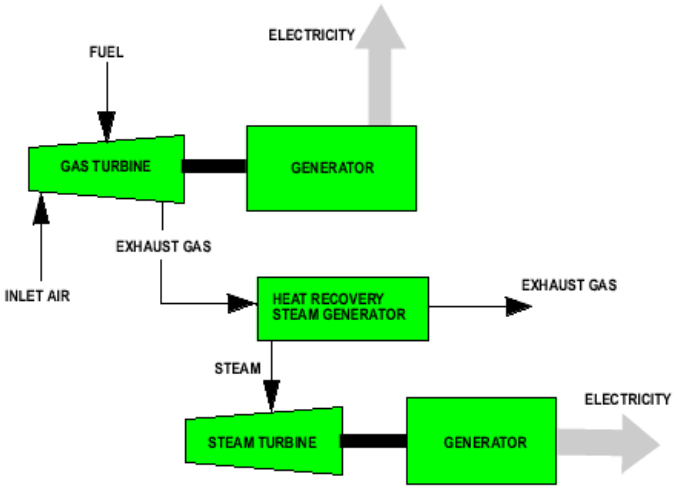

Figure 4 Schematic of a Combined-Cycle Plant

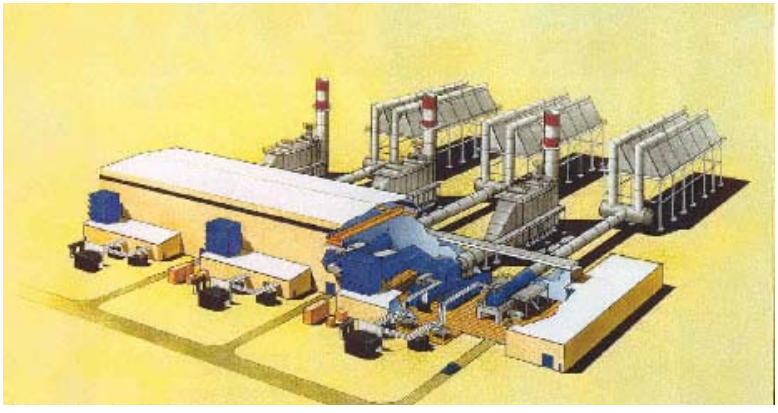

Figure 5 Artist's Rendering of the Modular Design of a Three-Unit, Combined-Cycle Plant

Internal Combustion Engine

An internal combustion engine burns diesel fuel to drive a generator to produce electricity. Diesel engines range in size from 50 kilowatts (kW) to 30 MW. They are typically used for peaking, emergency, or standby power. They generally use No. 2 diesel fuel oil, but they can also use heavy oil, low-grade kerosene, crude oil, and a variety of other liquids, such as coal liquids, shale oil, and vegetable oil. The main air pollutant from diesel engines using diesel fuel is NO_x. Depending on the duty cycle and state and federal environmental regulations, modifications may be required to the combustion process to reduce NO_x emissions. Diesel engines can be started and brought online very quickly. The time period from when a plant is ordered to when it is generating power can be as little as several days for very small units to about two years for large units.

Common Components of Fossil-Fuel Power Stations

Common components in a fossil-fuel power plant include fuel handling/treatment, processing unit, cooling unit, pollution control unit, power plant controls, and an onsite substation. The processing unit can include a combustor, boiler, turbine, and generator.

Fuel Handling/Treatment

Coal is delivered to a coal-fired generating plant site by railroad, ship, barge, and occasionally truck. It is placed in piles located outdoors as close to the plant as possible. For protection against annoyance and injury to the public as well as pilferage, coal piles are fenced in. For aesthetic reasons, however, in some cases the pile may be enclosed by a wall and landscaped. The top and sides of the pile are often sprayed with a thin layer of road tar or asphalt to seal the pile, preventing dust from becoming windblown and keeping out rain, moisture, and air. A base-loaded, coal-fired power plant may have a pile of coal sufficient to last for more than four months at 100% capacity.

Coal bunkers are installed as part of the plant structure not only to store a given quantity of coal but also to maintain a continuous supply of coal to the boiler furnaces. A bunker may hold a 24- to 48-hour supply of coal. Coal is brought from the outside coal pile by truck, dragline, conveyor, or other handling equipment. The bunker is the first stage of the process to prepare coal for combustion in the furnace. Coal must be crushed, pulverized, and screened before it can be burned. Figure 6 shows a coal-fired steam power plant with a coal pile and coal conveyor in the foreground.

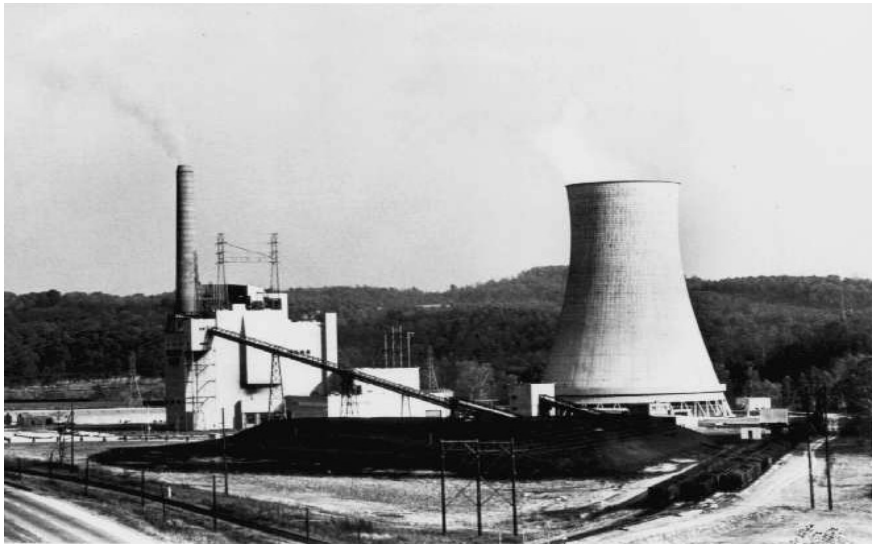

Figure 6 Coal Pile, Conveyor, and Natural Draft Cooling Tower at a Power Plant

Some coal-fired power plants using advanced technology (such as fluidized-bed combustion) may also use limestone in the combustion process to reduce emissions. Consequently, these plants would also have stockpiles of limestone at the plant site.

Natural gas is usually delivered by pipeline to a gas-fired power plant, but it can also be transported in liquefied form by railroad or ships. For economic reasons, pipelines are operated at or near capacity at all times. To meet fluctuations in natural gas demand at the power plant, storage facilities are located nearby. Such storage provides for demands beyond the pipeline capacity and periods when the pipeline is out of service.

Oil-fired power plants use tank farms located adjacent to the plant to store oil. The oil supply is usually stored in a number of tanks so that the loss or destruction of one or more tanks does not adversely affect plant operation. Each tank is enclosed inside an earthen or concrete coffer dam or well of sufficient height to contain the entire contents of the tank in the event of a tank leak or failure. Tanks are also located sufficiently far apart to protect against spread of fire. Tanks are painted in light colors to hold down temperatures and are not filled completely to allow for expansion and contraction of the oil as temperatures change. Before it is combusted, oil may need to be treated to remove high sulfur, salt, or metal content.

Processing Unit

The processing unit at a fossil-fuel power plant can contain the combustor, boiler, turbine, and generator appropriate for the type of unit, as previously described. These components are often enclosed in a building to protect them from the elements and facilitate repair and maintenance activities.

Cooling Unit

Steam and CC power plants use water for cooling. The source of cooling water can be a lake, cooling tower, or river. The cooling system used depends on the proximity of the power plant to a water source, the amount of heat that needs to be removed, and environmental regulations on the temperature difference of water discharged to the environment. Figure 2 shows an example of a mechanical draft cooling tower, whereas Figure 6 gives an example of a natural draft cooling tower. Natural draft cooling towers have become most often associated with nuclear power plants, but they are also used by large fossil-fired plants.

Combustion turbines typically do not have a separate cooling unit. Exhaust from the turbines is vented directly to the atmosphere, unless emissions regulations require that the exhaust be treated before being released.

Exhaust gases from a diesel engine are generally vented directly to the atmosphere. The radiator in a large diesel engine is usually cooled via a secondary circulating water system. Heat is dissipated to the atmosphere through an evaporative, mechanical draft cooling tower. A once-through cooling system can be used when the plant is located near a body of water and if environmental regulations allow. Air cooling of a radiator is used only for very small diesel engines.

Pollution Control Unit

Pollution controls are generally required for steam and CC power plants, depending on the type of fuel used and the environmental regulations. Pollution controls may also be required for combustion turbines and diesel generators, but to a lesser extent, because of their shorter duty cycle (they operate only a few hours per day). The types of pollution most often controlled are particulates, SO_2, and NO_x. Emissions are controlled in a variety of ways, including fuel selection (e.g., low-sulfur coal), fuel treatment (e.g., coal cleaning), combustion control (e.g., low-NO_x burners), and post-combustion control (e.g., limestone scrubbers). Post-combustion controls are usually the most visible pollution controls at a power plant. Higher flue gas stacks are often erected at power plants. The high stacks serve to dissipate the emissions over wide areas to reduce their effect at ground level.

Pollution controls are needed not only when a plant is built but also when a facility is expanded or improved. Under U.S. Environmental Protection Agency (EPA) rules, older plants that replace a limited portion of their equipment every year would be exempt from requirements to modernize their emission control systems, even if air pollutant emissions were increased as a result of the replacement. However, there is objection to the EPA rules because of concern over the increased pollution that could result.

Power Plant Controls

Power plants are operated from a centralized control room on the plant site. Control functions in power plants may be accomplished manually by operators, by automatic controls alone, or by combinations of manual and automatic controls. In many older plants, much of the operation is

accomplished manually by trained, skilled personnel. In newer plants, much of the data acquisition and most of the operations are performed automatically by mechanically or electronically actuated devices. In the newest plants, essentially all of the data acquisition and operations can be performed solely by computers. The increased use of automatic controls not only reduces the number of personnel needed to operate the plant but also permits rapid, detailed, and accurate correlation of operating conditions, which results in quicker response to changing conditions imposed on the generating plant.

In general, the smaller the plant, the fewer personnel it has. Some newer and smaller power plants in remote locations are fully automated and are visited only periodically for maintenance purposes. Other plants are operated semi-automatically from other stations via telephone and radio communication signals.

Onsite Substation

The onsite plant substation consists of a step-up transformer, switchgear, and transmission lines. The generation step-up transformer is usually located on the power plant site just outside the power plant building or adjacent to the plant site. This device transforms electric power produced by the turbine generators to the high voltage required by the transmission system. Generation step-up transformers are very large, expensive devices that are difficult and time-consuming to replace. Spares are not generally available.

Although not technically part of a power plant site, the switchgear and transmission lines that connect the plant to the electric grid are necessary for continuous operation of the plant. Any sudden loss of significant transmission capacity, whether by a downed tower or line or by destruction or disruption of a downstream substation, if large enough and at the right network location, could cause the plant to shut down and interrupt power production. Because these systems extend for miles outside the plant boundary and are not physically guarded, they are vulnerable.

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored regularly. Constant attention to these indicators can help 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 the 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 off-site computers. This type of data gathering might include 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 off-site access to the supervisory control and data acquisition [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 off-site 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 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 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 to 5 refer to activities not only in the immediate vicinity of the facility, but also activities within a relatively large region around the facility (e.g., 100 to 200 miles). Local authorities should be aware of such activities and 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 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 off-site 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, toxic, or radioactive materials.
12	Aircraft flyover in restricted airspace; 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., an electrical 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 off-site 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 all the time.
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 located 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 customer or vendor (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	A customer or vendor associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer or vendor 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 customer or vendor request for excessive confidentiality regarding the final destination or details of the product to be delivered.
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	Sale canceled by customer but then customer or vendor attempts to purchase or sell the exact same product with the same specifications and use but using a different name.
11	Sale canceled by customer or vendor but then the identical product is stolen or “lost” shortly after the customer’s or vendor’s inquiry.
12	Theft/loss/recovery of large amounts of cash by groups advocating violence against government/civilian sector targets (also applies to weapons of mass destruction).
	(Continued on next page.)

13	Customer or vendor does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
Customer/Vendor Behavioral Indicators: *What are customer or 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 activities.*	
14	Reluctance to give sufficient explanation of the materials to be produced with the equipment and/or the purpose or use of those materials.
15	Evasive responses.
16	Reluctance to provide information on the locations or place where the equipment is to be installed.
17	Reluctance to explain sufficiently what raw materials are to be used with the equipment.
18	Reluctance to provide clear answers to routine commercial or technical questions.
19	Reason for purchasing the equipment does not match the customer's or vendor's usual business or technological level.
20	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.
21	Unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
22	Plant, equipment, or item is said to be for a use inconsistent with its design or normal intended use, and the customer or vendor continues these misstatements even after being corrected by the company/distributor.
23	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.
24	Theft of material or equipment with no practical use outside of a legitimate business facility or industrial process.
25	Apparent lack of familiarity with nomenclature, processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in the business.
26	Discontinuity of information provided, such as a phone number for a business, but the number is listed under a different name.
27	Unfamiliarity with the "business," such as predictable business cycles, etc.
28	Unreasonable market expectations or fantastic explanations as to where the end product is going to be sold.

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.
Biological Agent Indicators:	
17	Sales or theft of large quantities of baby formula (medium for growth), or an unexplained shortage of it.
18	Break-ins/tampering at water treatment or food processing/warehouse facilities.
	(Continued on next page.)

19	Solicitation for sales or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities.
20	Persons stopped or arrested with unexplained lethal amounts of agents/toxins/ diseases/explosives.
21	Multiple cases of unexplained human or animal illnesses, especially those illnesses not native to the area.
22	Large number of unexplained human or animal deaths.
23	Sales (to non-agricultural users) or thefts of agricultural sprayers or crop-dusting aircraft, foggers, river craft (if applicable), or other dispensing systems.
24	Inappropriate inquiries regarding local or regional chemical/biological sales/storage/transportation points.
25	Inappropriate inquiries regarding heating and ventilation systems for buildings/facilities by persons not associated with service agencies.
26	Unusual packages or containers, especially near HVAC equipment or air-intake systems.
27	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
Radioactive Material Indicators:	
28	Break-ins/tampering at facilities storing radioactive materials or radioactive wastes.
29	Solicitation for sales or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities.
30	Persons stopped or arrested with unexplained radioactive materials.
31	Any one or more cases of unexplained human or animal radiation burns or radiation sickness.
32	Large number of unexplained human or animal deaths.
33	Inappropriate inquiries regarding local or regional radioactive material sales/storage/transportation points.

USEFUL REFERENCE MATERIAL AND RELATED WEB SITES

1. White House, *The 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. U.S. Federal Bureau of Investigation, *FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment* [http://www.vohma.com/pdf/pdffiles/SafetySecurity/ChemInfofbi.pdf]. This document includes a list of chemical/biological materials likely to be used in furtherance of WMD terrorist activities.

5. 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].

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

7. 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.

8. 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 elicitation, tests of security, acquiring supplies, suspicious persons out of place, dry run, and deploying assets.

9. 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].

10. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp].

11. Federal Bureau of Investigation [http://www.fbi.gov/].

12. Agency for Toxic Substances and Disease Registry [http://www.atsdr.cdc.gov/].

13. Centers for Disease Control and Prevention [http://www.cdc.gov/].

14. U.S. Department of Commerce, Bureau of Industry and Security [http://www.bis.doc.gov/].

15. National Museum of American History, *Throw the Switch: The Technology of Electric Power* [http://americanhistory.si.edu/csr/powering/backthrw.htm].

16. Edison Electric Institute [http://www.eei.org/].

17. U.S. Department of the Army, Technical Manual TM 5-811-6, *Electric Power Plant Design*, Jan. 20, 1984 (Chaps. 7 and 8) [http://www.usace.army.mil/publications/armytm/tm5-811-6].

18. Office of Energy, Queensland, Australia [http://www.energy.qld.gov.au/index.htm].

19. U.S. Department of Energy, Energy Information Administration [http://www.eia.doe.gov/].

20. CIPCO, *Fundamentals of Electricity* [http://cipco.apogee.net/foe/fg.asp].

21. Pansini, Anthony J., and Kenneth D. Smalling, *Guide to Electric Power Generation*, 2nd Ed., The Fairmont Press, Inc., 2002.

22. Rustebakke, Homer M., ed., *Electric Utility Systems and Practices*, 4th Ed., John Wiley & Sons, New York, 1983.

23. International Atomic Energy Agency, *Expansion Planning for Electrical Generating Systems, A Guidebook*, Technical Report Series No. 241, Vienna, Austria, 1984.

24. Kilian, Michael, "EPA Softens Rules to Allow More Emissions," *Chicago Tribune*, Section 1, p. 11, Aug. 28, 2003.

25. National Research Council, Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academies Press, Washington, DC, 2002.

26. North American Electric Reliability Council [http://www.nerc.com/].

27. U.S. Environmental Protection Agency [http://www.epa.gov/].

28. Right-to-Know Network [http://www.rtk.net/].