POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: HYDROELECTRIC DAMS

Protective Security Division
Department of Homeland Security

Draft Version 1.0, 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 hydroelectric dams.

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 hydroelectric dam 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.

HYDROELECTRIC DAMS BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to hydroelectric dams, it is useful to understand the basic structure of the industry and what general types of facilities might be attractive targets for terrorist attack. Hydroelectric dams are attractive terrorist targets because of the potential for dramatic effects of the destruction of a major dam, the potential for downstream damage and casualties from flooding, and the potential for impacts on the overall electric power grid from the loss of generating capacity, as depicted in Figure 1.

Damage or destruction of the facility can be intended to inflict casualties, both onsite and downstream; shut down or degrade the operation of the facility; or 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 the overall operation of the interconnected power grid. Theft of equipment or materials can be intended to divert them 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 for use in carrying out other attacks. Facility attacks can be intended to (1) cause economic, national security, or logistical harm; (2) disturb the overall grid operation; or (3) "weaponize" the facility against the surrounding human population by causing downstream flooding.

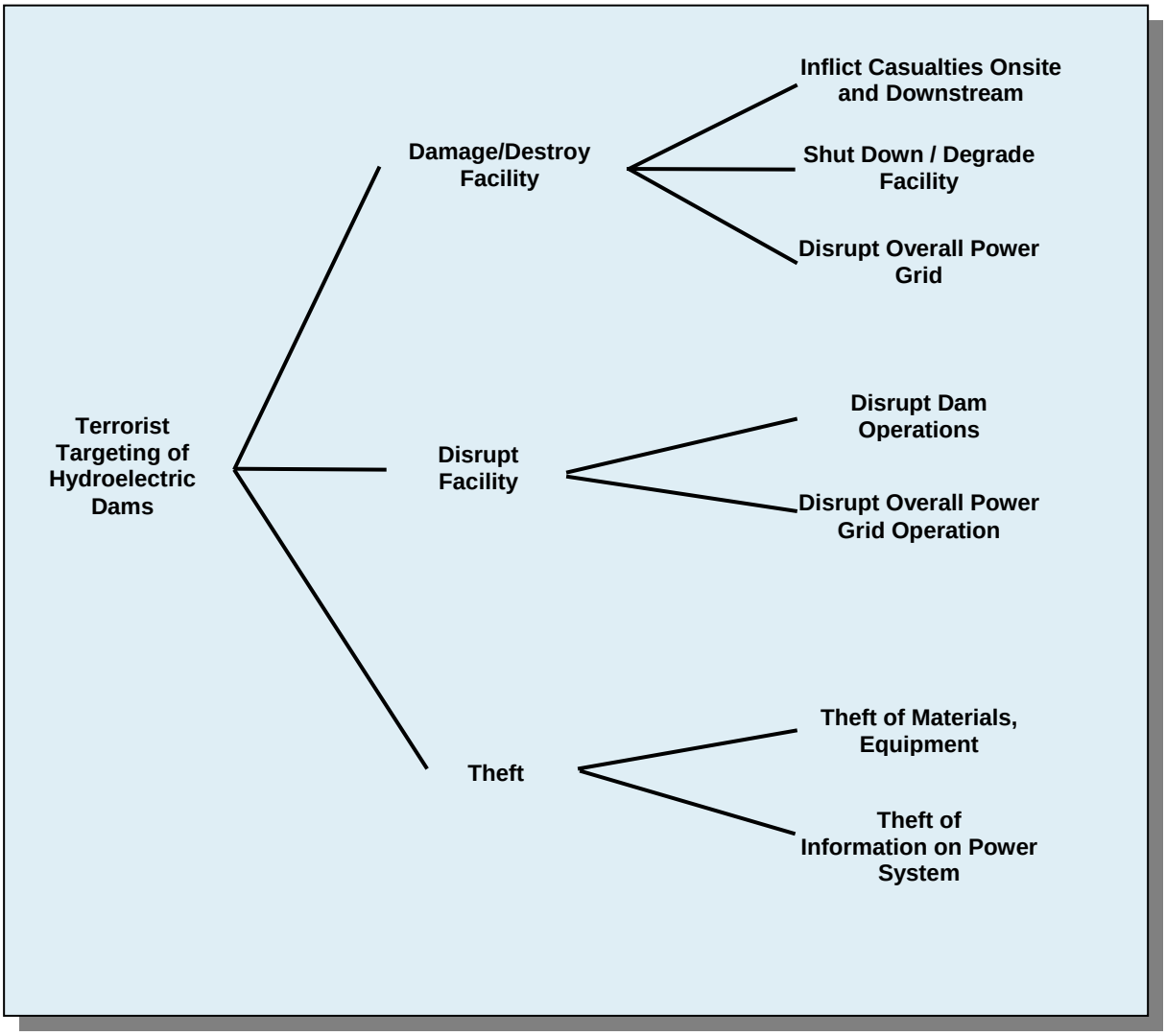

Figure 1 Terrorist Targeting Objectives

Sector Description

Hydropower, including pumped storage, constitutes about 14% of the electrical generating capacity of the United States (U.S.). Hydropower is the primary source of renewable energy in the U.S. The total U.S. hydroelectric capacity is 103.8 gigawatts (GW), including pumped storage projects. The federal government owns 38.2 GW at 165 sites (excluding pumped storage). Another 40 GW of non-federal, licensed conventional hydroelectric capacity (excluding pumped storage) exists at 2,162 sites in the U.S. (National Hydropower Association). Figure 2 illustrates the distribution of hydropower generating capacity by ownership. The 10 largest hydroelectric facilities in the country are listed in Table 1 (U.S. Society on Dams).

Federal ownership of hydroelectric facilities is concentrated in the U.S. Army Corps of Engineers (USACE), the U.S. Bureau of Reclamation (USBR), and the Tennessee Valley Authority (TVA).

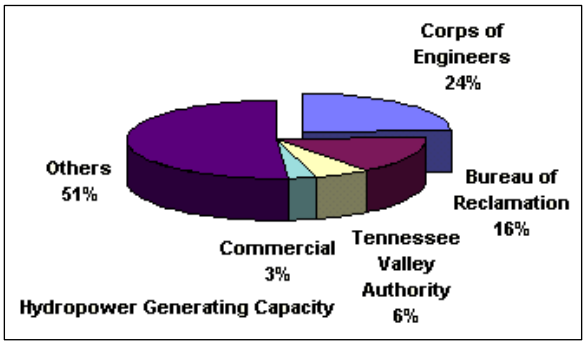

Figure 2 Distribution of Hydropower Generating Capacity (USACE)

Table 1 Ten Largest Hydro Projects in the United States

Dam	River	Location	MW
Grand Coulee	Columbia	Washington	6,180
Chief Joseph	Columbia	Washington	2,457
John Day	Columbia	Oregon	2,160
Bath County P/S	Little Back Creek	Virginia	2,100
Robert Moses - Niagara	Niagara	New York	1,950
The Dalles	Columbia	Oregon	1,805
Luddington	Lake Michigan	Michigan	1,657
Raccoon Mountain	Tennessee River	Tennessee	1,530
Hoover	Colorado	Nevada	1,434
Pyramid	California Aqueduct	California	1,250

Source: U.S. Society on Dams, *Register of Dams.*

The USACE is the largest hydropower producer, with 375 generating units and a total rated capacity of 21 GW. Its largest producer is the Bonneville Dam on the Columbia River, with 286 megawatts (MW) of rated capacity. Most of the USACE hydropower capacity is concentrated in the Northwestern Division, which, in addition to Bonneville, has 14 other dams with more than 100 MW of rated capacity (USACE Hydroelectric Design Center).

The USBR has somewhat less total hydropower capacity than USACE, with a total of 14.8 GW produced at 58 hydroelectric plants. The bulk of USBR's hydroelectric capacity, however, is concentrated in a few large dams. The top three dams account for more than two-thirds of capacity: Grand Coulee (6.8 GW), Hoover (2 GW), and Glen Canyon (1.3 GW).

The TVA maintains 29 conventional hydroelectric dams throughout the Tennessee River system and 1 pumped-storage facility for the production of electricity. TVA hydroelectric facilities have a total capacity of about 5 GW. Its largest facility is the Raccoon Mountain pumped storage reservoir with 1.5 GW of capacity. Altogether, TVA operates 15 dams with more than 100 MW of hydroelectric generating capacity. In addition, 4 Alcoa dams on the Little Tennessee River and 8 Corps of Engineers dams on the Cumberland River contribute to the TVA power system.

Most non-federal hydroelectric dams are operated by power companies and are licensed by the Federal Energy Regulatory Commission (FERC). FERC listed 1,010 licensed hydroelectric facilities in 2001 (FERC). Of the licensed facilities, 14 are 1 GW or more in size; the largest (2.75 GW) is the Niagara facility, which is owned by the New York Power Authority.

Actual generation supplied by hydropower facilities varies from year to year depending on rainfall and other factors, but it is generally somewhat less than 10% of the total for the U.S. For example, hydropower supplied 8.5% and 7.2% of the electricity generated in the U.S. in 1999 and 2000, respectively. In some states, however, the percentage is much higher, primarily in the western U.S. Table 2 shows the 10 states most reliant on hydropower production in 2000 (U.S. Energy Information Administration).

The hydroelectricity currently produced each year in the U.S. is equivalent to nearly 500 million barrels of imported crude oil. This total represents a value for existing hydrogenation of about $9 billion annually. Hydropower generation does not produce atmospheric emissions, which are a growing problem on both national and global levels (USBR).

Hydroelectric facilities come in many shapes and sizes; however, they all have certain features in common. A dam is built on a river to provide a reservoir of water that is at a higher elevation than the flow downstream. The potential energy of this water is released in a controlled fashion as the water is allowed to run from the reservoir through tunnels or pipes, which are referred to as penstocks, driving one or more turbines connected to generators. After driving the turbines, the water is released downstream. A gate is used to control the flow through the penstocks. Figure 3 illustrates the key features of a hydroelectric dam.

Table 2 Ten States Most Reliant on Hydropower Production in 2000

State	Hydropower Percentage of Electricity Production (%)
Idaho	92
Washington	74
Oregon	74
South Dakota	59
Montana	42
Maine	29
Vermont	20
California	19
New York	18
Alaska	16

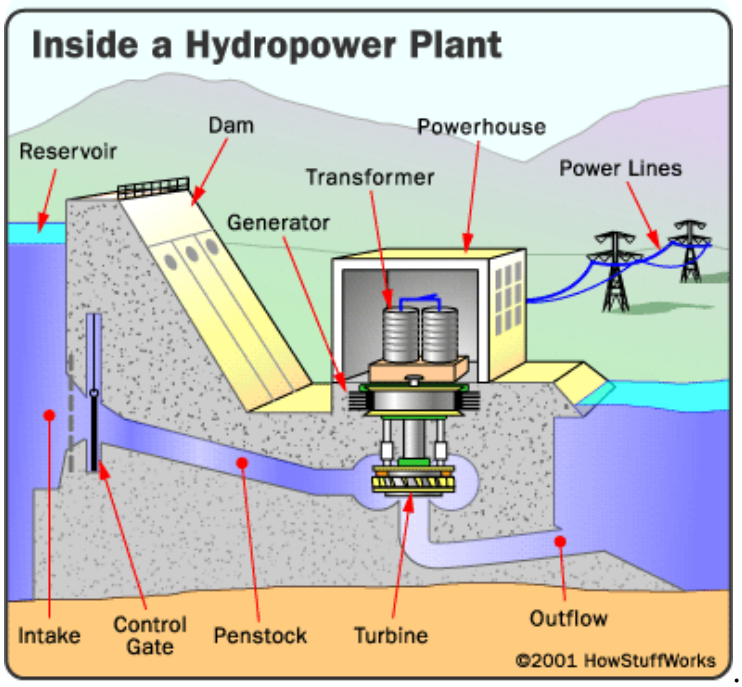

Figure 3 Key Features of a Hydroelectric Dam

Hydroelectric dams typically release water from the reservoir in a controlled manner that bypasses the electricity-generating facility. A bypass may be necessary to allow work on the turbines, to release extra water in times of flood, or to maintain stream flow. The bypass can be in the form of additional penstocks or one or more spillways that allow water to flow over the top of the dam. Flow through the bypasses is controlled by gates and valves. In general, each dam

uses electromechanical devices to control water flow through the facility from a central control room using a supervisory control and data acquisition (SCADA) system.

Some hydroelectric facilities have a pumped-storage facility to store water for release as needed to meet electrical demand. A pumped-storage facility uses two reservoirs; one is located at a higher elevation than the other. During periods of low demand for electricity, such as nights and weekends, energy is stored by reversing the turbines and pumping water from the lower to the upper reservoir. When electrical demand is high, the stored water can be released to turn the turbines and generate electricity as it flows back into the lower reservoir.

Many hydroelectric dams, especially the larger ones, have multiple missions. Besides producing electricity, they can provide:

- Water supply for human domestic consumption, industrial uses, and agricultural irrigation;
- Flood control and river navigation;
- A transportation link for vehicular traffic (across the top of the dam); and
- Water-based recreational uses (boating and fishing).

In the arid western U.S., in particular, the water supply and irrigation functions of larger dams can be significant. Grand Coulee Dam in eastern Washington State provides irrigation for more than 500,000 acres of the Columbia River Basin from Coulee City in the north to Pasco in the south. At its maximum height, Lake Mead—the reservoir formed by blocking the Colorado River at Hoover Dam—covers 247 square miles with 28,537,000 acre-feet of water, which is equivalent to two years of average flow of the river. Water is apportioned from the Colorado River system per agreements and treaties to seven states and Mexico with a total allotment of 16.5 million acre-feet per year. Lake Mead is the primary source of domestic water for Las Vegas and is a major source for Los Angeles, San Diego, and other southern California communities, as well as for agricultural irrigation in southern California and Nevada.

A key mission of essentially every dam is flood control. Failure of flood control at a major hydroelectric dam is likely to lead to property damage and loss of life downstream. Note that a flood control failure does not necessarily require a catastrophic failure of the dam; it can also result from manipulation or failure of the SCADA system or the gates and valves it operates, allowing more water than desired to exit the reservoir.

Dams are built according to well-documented engineering principles and regulated standards. They are designed to withstand a variety of potential problems: inherent structural flaws; failure of materials used to construct the dam; aging and deterioration; failure of the land that supports the dam; cracking caused by earthquakes or the natural settling of the dam; inadequate monitoring and maintenance; sink holes in the dam; and excessive flooding and landslides. A well-built large dam is difficult to destroy. Philip Anderson of the Center for Strategic and International Studies in Washington, DC, remarked, "Even in wartime, the military has a hard time breaking through the larger dams. It would be tremendously difficult for terrorists to carry enough explosives with them to destroy a large dam" (*News Journal*).

Typically, dams appeal to many visitors. The reservoirs associated with hydroelectric dams are often recreational facilities that attract large numbers of people for leisure activities, such as boating, fishing, and swimming. In some cases, the dam is considered to be a tourist attraction. In 2000, Hoover Dam recorded 1,276,292 visitors; in 2002, Glen Canyon Dam and Lake Powell had more than 2 million visitors (Friends of Lake Powell). The large number of visitors to these facilities can complicate security procedures.

The consequences of the disruption of a hydroelectric dam depend a great deal on the dam and the specific circumstances of the event. Disruption of electrical generation or transmission equipment could lead to short- or long-term removal of the dam's electric-generating capacity. Some equipment could take months to replace. Local or regional electric power grids could be affected depending on demand and the size and duration of the supply disruption. About 20 hydroelectric plants have a capacity of 1 GW or more; the rest are smaller. For most of the larger hydroelectric facilities, removal of the facility from service would have an impact roughly equivalent to removal of a large- or moderate-sized fossil fuel or nuclear plant.

Because hydroelectric facilities generally serve multiple missions, their disruption can cause multiple effects. Besides loss of electric-generating capacity, effects can include loss of water supply for domestic and irrigation purposes, flooding, and damage to transportation facilities. As noted above, failure of the flood control mission of a dam can result from disruption or manipulation of the facility's control mechanisms, as well as from physical destruction of the dam.

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 of 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 off-site 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 off-site 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 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 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 hydroelectric dam; 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 facility, but also to activities within a relatively large region around the plant (e.g., 100 to 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 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 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 (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 associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer 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 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 attempts to purchase the exact same product with the same specifications and use but using a different name.
11	Sale canceled by customer but then the identical product is stolen or “lost” shortly after the customer’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).
13	Customer does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
	(Continued on next page.)

Customer Behavioral Indicators: *What are customer behavioral indicators? Actions or inactions on the part of a customer for equipment or materials that appear to be inconsistent with normal behavioral patterns expected from legitimate commercial customers.*	
14	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.
15	Evasive responses.
16	Reluctance to provide information on the plant 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 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 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, chemical processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in purchasing chemicals.
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.
	(Continued on next page.)

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.
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 heating, ventilating, and air-conditioning (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

1. The 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. 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 surveillance, 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. Association of State Dam Safety Officials (ASDSO) [http://www.damsafety.org].

11. Congressional Research Service, 2002, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, Feb. 7 [http://carper.senate.gov/acrobat%20files/RS21026.pdf].

12. Federal Energy Regulatory Commission (FERC), hydropower page [http://www.ferc.gov/industries/hydropower/gen-info.asp].

13. Federal Emergency Management Agency (FEMA), National Dam Safety Program [http://www.fema.gov/fima/damsafe/ndspact.shtm].

14. Federal Guidelines for Dam Safety: Selecting and Accommodating Inflow Design Floods for Dams [http://www.fema.gov/fima/damsafe/idf_toc.shtm].

15. Federal Dam Safety and Security Act of 2002, P.L. 104-303 [http://thomas.loc.gov/].

16. Friends of Lake Powell [http://www.lakepowell.org/].

17. Hallett, Amber, *Hydropower: Environment, Safety, and Politic*s [http://www.physics.pomona.edu/phys17/papers/HydroEnv&Pol.pdf].

18. Institute for Dam Safety Risk Management, Utah Water Research Laboratory, Utah State University, Logan [http://www.engineering.usu.edu/uwrl/idsrm.htm].

19. National Hydropower Association [http://www.hydro.org/hydrofacts/facts.asp].

20. National Performance of Dams Program, Stanford University [http://npdp.stanford.edu/index.html].

21. U.S. Army Corps of Engineers [http://www.usace.army.mil].

22. U.S. Army Corps of Engineers, Hydroelectric Design Center [https://www.nwp.usace.army.mil/hdc/].

23. U.S. Department of the Interior, Bureau of Reclamation, Teton Basin Project [http://www.usbr.gov/dataweb/html/teton1.html].

24. U.S. Energy Information Administration [http://www.eia.doe.gov/cneaf/electricity/page/pubs.html].

25. United States Society on Dams, Dams, Hydropower, and Reservoir Statistics [http://www.ussdams.org/uscold_s.html].

26. Witherspoon, Roger, "U.S. Reconsiders Terrorist Targets," *Journal News*, March 30, 2003 (original publication date) [http://www.thejournalnews.com/newsroom/033003/a0130warsecurity.html].

RELATED WEBSITES

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

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

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

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

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