# POTENTIAL INDICATORS OF TERRORIST ACTIVITY
# INFRASTRUCTURE CATEGORY: CABLE LANDING STATIONS

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 cable landing stations, which carry about 95% of all intercontinental telecommunications traffic (voice, data). These stations and associated cables form the backbone for international banking, finance, and commerce transactions and the Internet. Cable landing stations, which are often located near populated areas, are particularly vulnerable to attack.*

## 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 and what it might look like. The key factor to early recognition of terrorist activity is the ability to recognize anomalies in location, timing, and character of vehicles, equipment, people, and packages in proximity to sensitive areas.

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. Due to the relatively small number of cable landing stations present in the United States (U.S.), which when combined carry 95% of intercontinental voice/data traffic, a coordinated multi-target attack could severely disrupt intercontinental communications for an extended period of time, especially if combined with disruption of satellite communications.

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.

## CABLE LANDING STATION BACKGROUND

### Terrorists Targeting Objectives

Terrorists or terrorist groups may target cable landing stations to (1) cause bodily harm or death and/or (2) cause serious economic harm, as depicted in Figure 1. Bodily harm or death could be accomplished by a direct attack on a cable landing station either by using explosive devices, chemical weapons, biological weapons, or radiological weapons, or by releasing hazardous materials at the landing station, thereby potentially affecting station employees and contractor personnel, as well as third parties at the facility and on adjacent sidewalks and streets. Serious economic harm could be accomplished through direct damage and destruction of the landing station as a result of interruptions or shutdowns of telecommunication systems. Use of chemical, biological, or radiological weapons could cause lengthy delays in repairing the damage due to the necessity of removing contamination before crews could access the damaged components, or through relocating operations at another location.

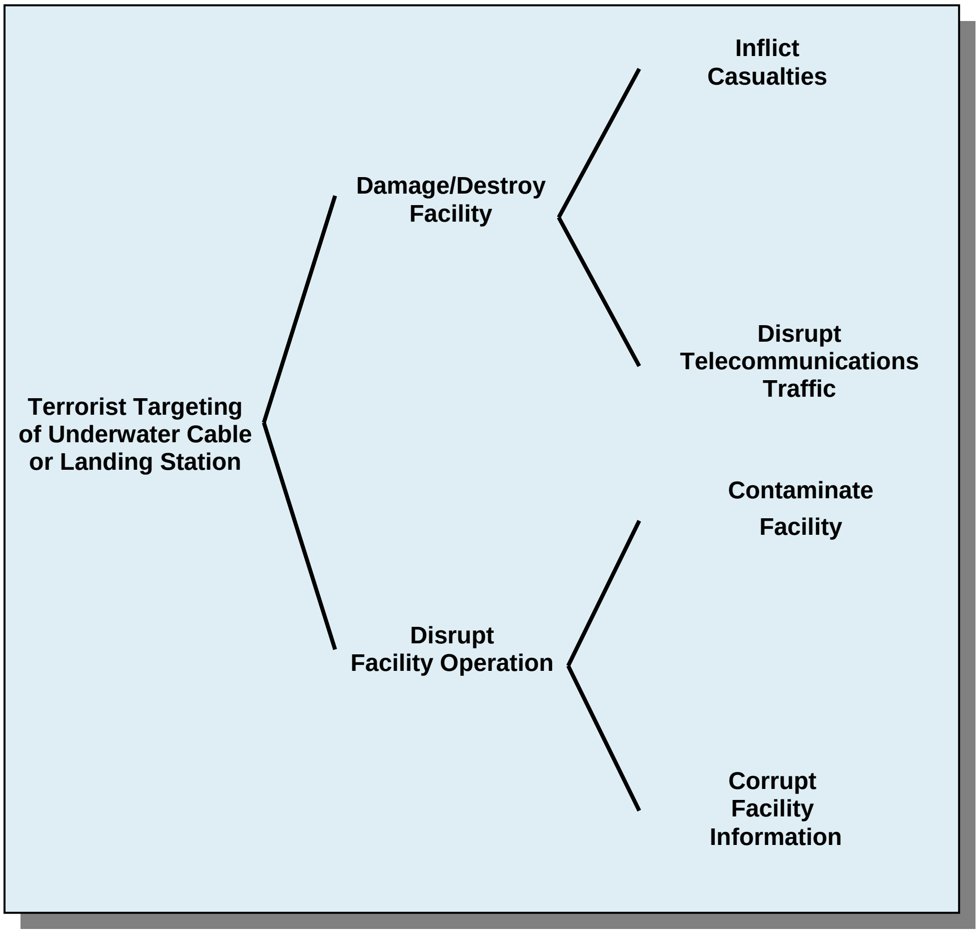

Terrorist Targeting of Underwater Cable or Landing Station
Damage/Destroy Facility
Disrupt Facility Operation
Inflict Casualties
Disrupt Telecommunications Traffic
Contaminate Facility
Corrupt Facility Information

**Figure 1 Terrorist Targeting Objectives for Underwater Cables/Landing Stations**

## Sector Description

Underwater cables carry telecommunications traffic (voice and data) under bodies of water (e.g., lakes and seas). These cables carry about 95% of all intercontinental telecommunications traffic. International banking and finance transactions are highly dependent on underwater (also known as submarine) communications cables. Some military communications traffic is carried via underwater cables. Most underwater communications cables in service are fiber-optic cables. New systems are almost always equipped with fiber-optic cables (rather than old-technology, coaxial cables). Underwater cable systems have expanded in recent years due to increased demand, changes in technology, and reduction in costs. This report focuses on the gateway point to underwater cable systems, the cable landing station, including the fiber run from the station to shore where the fiber enters the water. Additional detail on the underwater portion of fiber cabling can be found in *Characteristics and Common Vulnerabilities, Infrastructure Category: Underwater Cables*, Draft, December 15, 2003.

In deep water, the cable lies on the floor of the lake or sea. Long-distance telecommunication cables require repeaters to maintain a high signal-to-noise ratio and minimize signal degradation. Supervisory functions help diagnose cable performance and detect and locate faults. In shallow waters, the cable may be buried to minimize the possibility of damage from ship anchors and commercial and recreational maritime activities. On land, a cable terminates in a cable landing station, which contains power feed and terminal equipment. The terminal equipment routes the traffic to its next destination, which could be another underwater cable or a telephone switching system.

Submarine cables enter the continental U.S., Hawaii, and Alaska at various locations as shown in Figure 2. Each of the cable landing locations has a number of redundant and diverse backhaul routes. These routes provide connectivity on both regional and local levels between the cable landings and the domestic network. Table 1 lists 52 cable landing stations in the U.S. The majority of these landing sites use fiber optics.

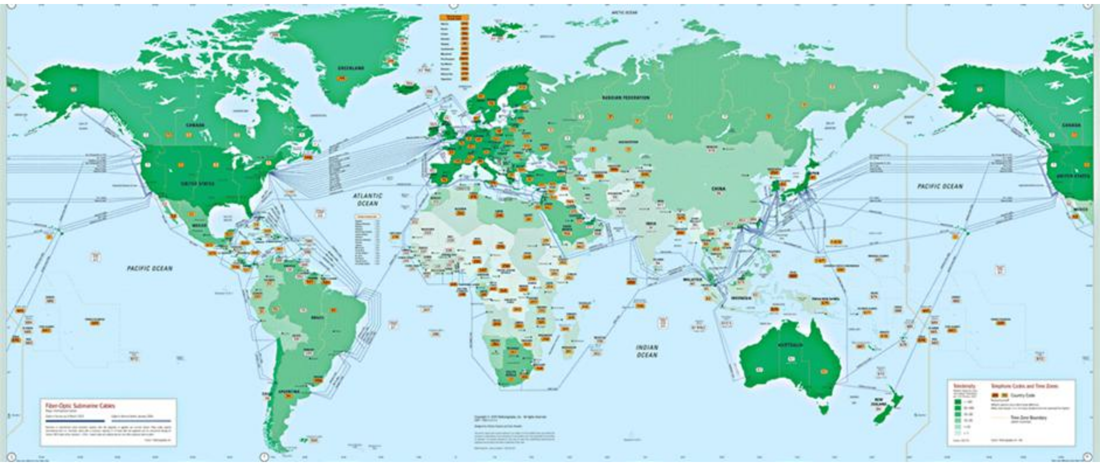


**Figure 2 Underwater Cables**

Although there are a number of locations and cables and the data flow can usually be dynamically re-routed in the event of secondary single path losses, the usage or capacity is not evenly distributed. Figure 3 shows that the largest data pipes are currently between New York and the United Kingdom.

Figure 4 shows an end-to-end schematic for an underwater telecommunications cable. One or more landing stations are associated with each end of a cable. Landing stations comprise the "dry plant," and a cable and its components comprise the "wet plant" for a cable system. Communications traffic flows between landing stations.

**Table 1 U.S. Cable Landing Locations**

| City | State | City | State | City | State |
|---|---|---|---|---|---|
| Lynn | MA | Seward | AK | Moss Landing North | CA |
| Green Hill | RI | Juneau | AK | Moss Landing South | CA |
| Shirley | NY | Whittier | AK | San Luis Obispo | CA |
| Brookhaven | NY | Valdez | AK | Grover Beach | CA |
| New York City | NY | Harbour Pointe | WA | Hermosa Beach | CA |
| Far Rockaway | NY | Seattle | WA | Kahe Point | HA |
| Arverne | NY | Lynnwood | WA | Lualualei | HA |
| Manhattan Beach | NY | Nedonna Beach | OR | Makaha | HA |
| Mastic Beach | NY | Coos Bay | OR | Lihue | HA |
| Crab Meadow Beach | NY | Pacific City | OR | Keawaula | HA |
| Long Beach | NY | Bandon | OR | Spencer Beach | HA |
| Manahawkin | NJ | Twin Rocks | OR | Ko Olina | HA |
| Manasquan | NJ | Hillsboro | OR | Koko Head | HA |
| Tuckerton | NJ | Manchester | CA | Kihei | HA |
| Wall Township | NJ | Point Arena | CA | Kawaihae | HA |
| Boca Raton | FL | Morro Bay | CA | Sandy Beach | HA |
| Hollywood | FL | Monterey Bay | CA | Manele Bay | HA |
| North Miami Beach | FL | | | | |

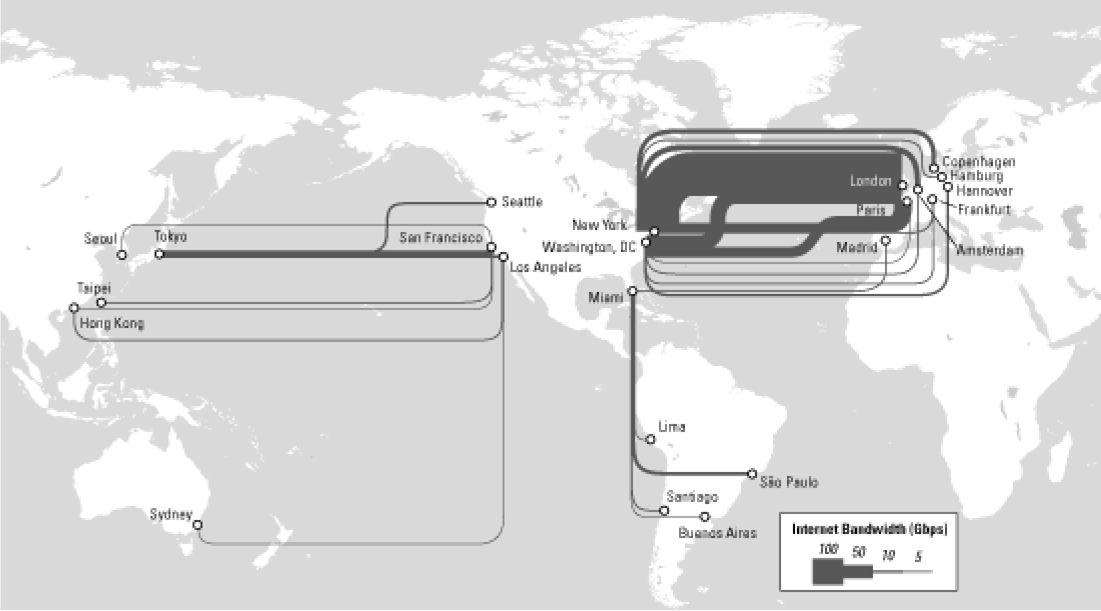
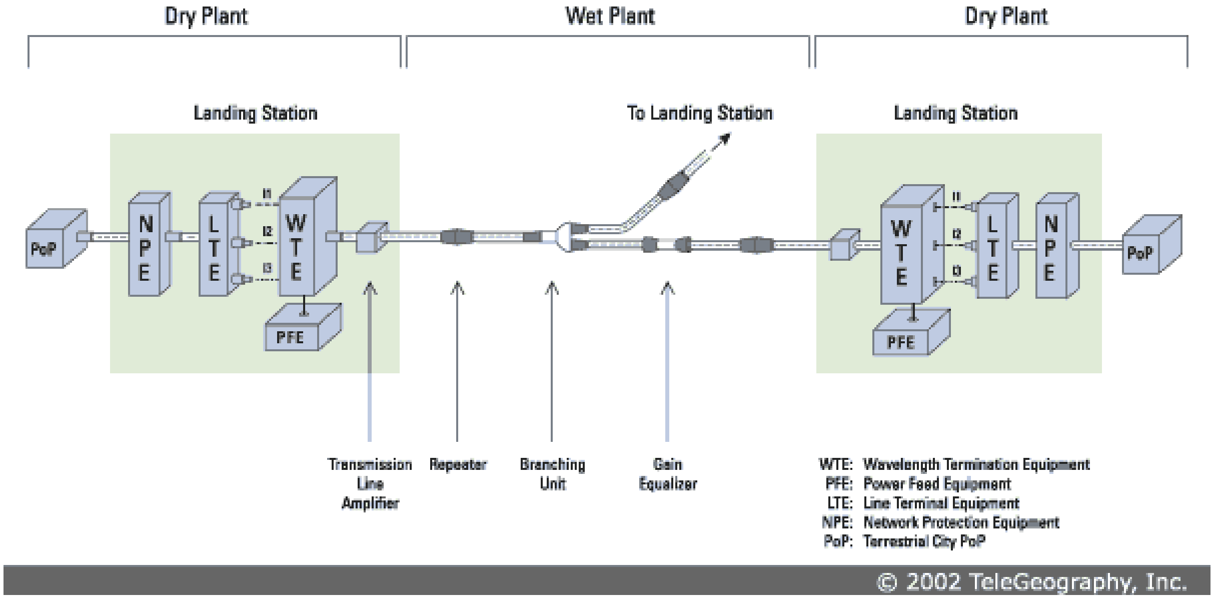


**Figure 3 Map of Major Interregional Internet Routes, 2003**


Dry Plant
Wet Plant
Dry Plant
Landing Station
To Landing Station
Landing Station
PoP
NPE
LTE
WTE
l1
l2
l3
PFE
WTE
LTE
NPE
PoP
PFE
Transmission Line Amplifier
Repeater
Branching Unit
Gain Equalizer
WTE: Wavelength Termination Equipment
PFE: Power Feed Equipment
LTE: Line Terminal Equipment
NPE: Network Protection Equipment
PoP: Terrestrial City PoP

© 2002 TeleGeography, Inc.

**Figure 4 End-to-End Schematic for a Transcontinental Telecommunications Connection**

The dry plant, which is typically housed in a cable landing station, includes the following components:

- Network protection equipment (NPE),
- Line terminal equipment (LTE),
- Wavelength termination equipment,
- Transmission line amplifiers,
- Circuitry for supervisory functions (cable performance, fault detection, and location),
- Power-feed equipment, and
- Terrestrial city point-of-presence—a site with a collection of telecommunications equipment (usually modems, digital leased lines, and multi-protocol routers).

At the cable landing station, terminal equipment (NPE, LTE) is installed and connected to the land-side (domestic) communications network. The intercontinental fiber is brought on-shore and is typically trenched (Figure 5) or routed along rights-of-way, such as along bridges and railways.

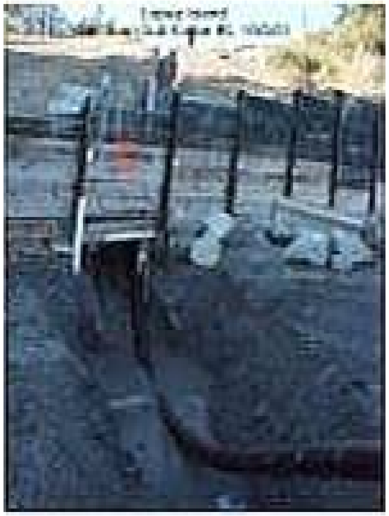


**Figure 5 On-shore Cable Trench**

The wet plant includes the following:

- Repeaters,
- Branching units (to allow one transoceanic cable to connect to more than one landing station),
- Supervisory circuitry, and
- Gain equalizers.

In the continental U.S., cable entry points are spread across the West Coast from Washington to California; along the East Coast, however, entry points are concentrated in an area from New Jersey to Connecticut and in another area around Miami, Florida. Cable landing stations are often situated close to populated areas, and precise cable landing positions are often publicly available on the Internet and elsewhere.

Cable providers typically use a fully redundant system architecture (such as alternate cables, connection to multiple international switches and landing locations, and satellite links). Hence, a system can sustain multiple points of failure without loss of connectivity.

At present, there are basically no restrictions on laying submarine cables in the high seas and on continental shelves; however, each country has jurisdiction over its territorial waters, and many impose regulations. In the U.S., cables and cable landings are under the jurisdiction of the Federal Communications Commission and the U.S. Environmental Protection Agency (National Environmental Policy Act of 1969 [42 USC 4321-4327]). The U.S. Department of State also has a role.

# 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 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 improves 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, global positioning systems, and cellular phones. It should be assumed that many terrorists have access to high-dollar 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 such information as site maps, locations of key facilities, 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 an accident by opening or closing a track switch using off-site access to a 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 (if feasible) 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 cable landing station or readily accessible routing of the transcontinental fiber cable; most of the other indicator categories in this report address activities in a much larger region around the underwater cable facility that should be monitored.

### 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 underwater cable station, but also activities within a relatively large region around the station (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 anywhere along the communications path 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 | Nonmilitary 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 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 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. |
| 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 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 locations of the plant 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. |

## 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 of 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 nonagricultural purchasers or abnormally large amounts to agricultural purchasers. |
| 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 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. |

| | |
|---|---|
| **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. |
| **Chemical Agent Indicators:** | |
| 8 | Inappropriate inquiries regarding local chemical sales/storage/transportation points. |
| 9 | Purchase or theft of explosives or restricted or sensitive chemicals. |
| 10 | Rental of self-storage units and/or delivery of chemicals to such units. |
| 11 | Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units. |
| 11 | Treated or untreated chemical burns or missing hands and/or fingers. |
| 12 | Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems. |
| 13 | Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems. |
| | (Continued on next page.) |

| | |
|---|---|
| **Biological Agent Indicators:** | |
| 14 | Sales or theft of large quantities, or an unexplained shortage in the area of baby formula (medium for growth). |
| 15 | Break-ins/tampering at water treatment or food processing/warehouse facilities. |
| 16 | Solicitation for sales or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities. |
| 17 | Persons stopped or arrested with unexplained lethal amounts of agents/toxins/ diseases/explosives. |
| 18 | Multiple cases of unexplained human or animal illnesses, especially those illnesses not native to the area. |
| 19 | Large number of unexplained human or animal deaths. |
| 20 | Sales (to nonagricultural users) or thefts of agricultural sprayers or crop dusting aircraft, foggers, river craft (if applicable), or other dispensing systems. |
| 21 | Inappropriate inquiries regarding local or regional chemical/biological sales/storage/transportation points. |
| 22 | Inappropriate inquiries regarding heating and ventilation systems for buildings/facilities by persons not associated with service agencies. |
| 23 | Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems. |
| 24 | Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems. |
| **Radioactive Material Indicators:** | |
| 25 | Break-ins/tampering at facilities storing radioactive materials or radioactive wastes. |
| 26 | Solicitation for sales or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities. |
| 27 | Persons stopped or arrested with unexplained radioactive materials. |
| 28 | Any one or more cases of unexplained human or animal radiation burns or radiation sickness. |
| 29 | Large number of unexplained human or animal deaths. |
| 30 | Inappropriate inquiries regarding local or regional radioactive material sales/storage/transportation points. |

## USEFUL REFERENCE MATERIAL

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

2. *Terrorist Attack Indicators*. The html version is available at http://afsf.lackland.af.mil/ Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack% 20Indicators. The PDF version of the file is available at 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 =UT-8.

3. U.S. Department of Homeland Security, *Potential Indicators of Threats Involving Vehicle Borne Improvised Explosive Devices (VBIEDs)*, Homeland Security Bulletin, May 15, 2003, available at 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*, available at 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*, available at 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?*, available at http://web.princeton.edu/sites/publicsafety/.

7. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents*, available at 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*, available at 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, available at http://www.homelanddefensejournal.com/archives/pdfs/ Feb_12_vol2_iss3.pdf.

## RELATED WEBSITES

1. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp], accessed Aug. 11, 2003.
2. Federal Bureau of Investigation [http://www.fbi.gov/], accessed Aug. 14, 2003.
3. U.S. Environmental Protection Agency [http://www.epa.gov/], accessed Aug. 11, 2003.
4. U.S. Department of State [http://www.state.gov/], accessed Aug. 13, 2003.
5. Federal Electric Regulatory Commission [http://www.ferc.gov], accessed Aug. 14, 2003.
6. United Nations [http://www.un.org/], accessed Aug. 13, 2003.
7. Oregon Fishermen's Cable Committee [http://www.ofcc.com], accessed Aug. 11, 2003.
8. The International Cable Protection Committee [http://www.iscpc.org], accessed Aug. 14, 2003.
9. Global Marine Systems [http://www.globalmarinesystems.com], accessed Aug. 11, 2003.
10. KDDI-SCI [http://www.kddiscs.co.jp/e/business/02.html], accessed Aug. 11, 2003.
11. Makai Ocean Engineering Inc. [http://www.makai.com], accessed Aug. 11, 2003.
12. Global Crossing [http://www.globalcrossing.com], accessed August 11, 2003.
13. Neptune Regional Electrical Transmission System [http://www.neptunerts.com], accessed Aug. 11, 2003.
14. The International Cable Protection Committee [http://www.iscpc.org], accessed Aug. 13, 2003.
15. Federal Electric Regulatory Commission [http://www.ferc.gov], accessed Aug. 14, 2003.
16. John Young's Eyeballing Series [http://cryptome.org/cable-eyeball.htm], accessed Aug. 14, 2003.
17. Compagnie Financière Alcatel [http://www.alcatel.com/submarine/index.htm], accessed Aug. 11, 2003.
18. Telegeography [http://www.telegeography.com], accessed Aug. 12, 2003.