# POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: ELECTRIC POWER SUBSTATIONS

Protective Security Division
Department of Homeland Security

DRAFT – Version 1.0, December 15, 2003

*Preventing terrorism and reducing the nation's vulnerability to terrorist acts requires 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 electric power substations.*

## 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 substation 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" the unusual activities, incidents, and behaviors highlighted in this report.

## ELECTRIC POWER SUBSTATIONS BACKGROUND

### Terrorist Targeting Objectives

To consider terrorist threat indicators in relationship to electric power substations, it is useful to understand the basic structure of the industry and what general types of facilities might be attractive targets for terrorist attack. Electric power substations are attractive terrorist targets because the loss of electric power has both direct and indirect impacts. Direct impacts include, for example, interruption of home and commercial building heating or cooling, damage to electronic data and equipment, the inability to operate life-support systems in hospitals and homes, and damage to the electric grid. Without electric power, other critical infrastructures, such as transportation, water supply systems, telecommunications, and banking and finance, cannot function. Indirect impacts may also include fatalities, injuries, and expenses related to failures in these interdependent infrastructures. Terrorist targeting objectives for electric power substations are depicted in Figure 1.

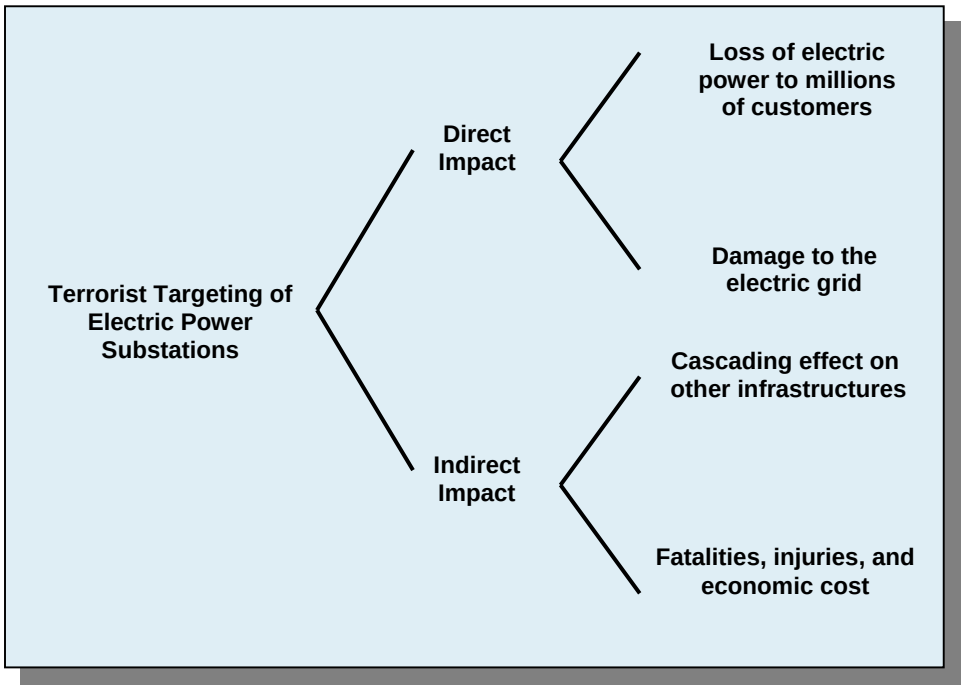


**Figure 1 Terrorist Targeting Objectives for Electric Power Substations**

## Sector Description

### *Common Electric Power Substation Characteristics*

The electric power substation is a principal component of the electrical transmission and distribution (T&D) infrastructure. It is a facility for switching electrical elements, transforming voltage, regulating power, and metering. A high-voltage substation typically includes an arrangement of components that are used to transform electric power during its transmission from generation to load. Depending on its location within the electrical network, a substation can support the transmission, distribution, or T&D infrastructure(s). This report focuses on T&D substations.

There are two basic types of power lines: transmission lines and distribution lines. Transmission lines are high-voltage power lines. The high voltage makes it possible to carry electric power efficiently over long distances from electrical generation facilities to substations near load centers. In the United States (U.S.), most transmission lines use alternating current (AC) and operate at voltages between 69 and 765 kilovolts (kV) (1 kV = 1,000 volts [V]).

Utilities use lower-voltage distribution lines to bring power from substations to businesses and homes. Distribution lines operate at voltages of less than 69 kV. Different customer classes receive electricity at different voltage levels from the distribution system. Some industrial customers receive electricity at 13 kV. For residential customers, these levels are further reduced to 120/240 V once the power reaches the neighborhood of its destination.

Transmission and distribution substations serve many functions associated with controlling and transferring power in an electrical system. Transmission substations usually have several incoming and outgoing transmission lines joined through arrangements of major electrical connections (buses) having very high-speed circuit breakers (used to disconnect lines). Several types of equipment can be used, depending on the functions of the particular substation. Transformers change the high voltages between different transmission voltage levels and between transmission lines to the lower voltages used by distribution lines. Together, many facilities make up an electric power system, as indicated in Figure 2.

As an integral part of the electric power infrastructure, the substation functions as a connection and switching point for transmission lines, distribution feeders, generating units, transformers, and other electrical equipment required to operate the system. As a result, substations are designed to provide reliability, flexibility, and continuity of service at the lowest investment costs that satisfy system requirements. Because system reliability is a key factor in considering substation design alternatives, the vulnerability of substations and their associated equipment make them vitally important to the electric power infrastructure.

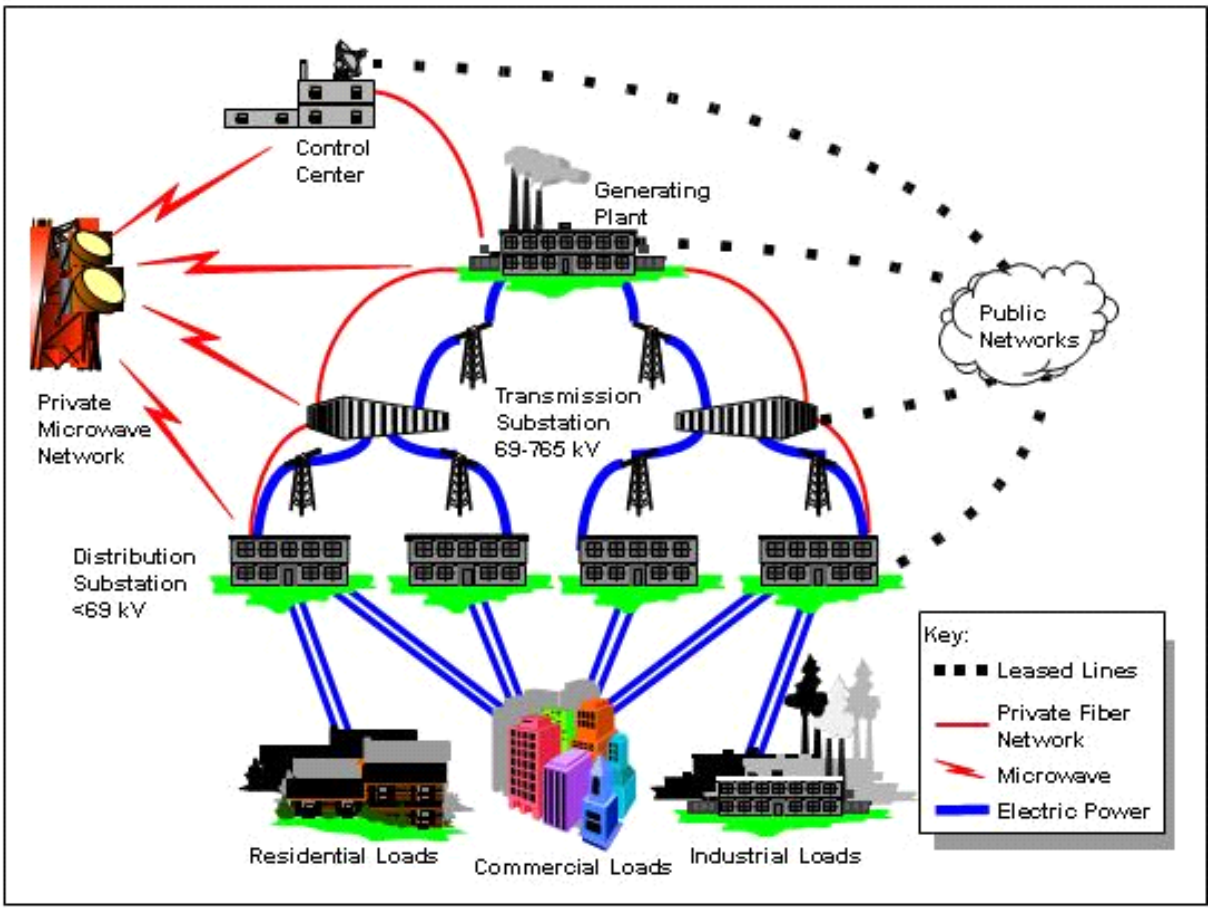


**Figure 2 Overview of the Electric Power System and Control Communications**

***Common Components***

Figure 3 shows the general layout of a T&D substation. Figure 4 presents a simplified view of connectivity in the electric power system. Of course, the supply of electricity to industrial, commercial, and residential loads comes from the interconnected electric grid and not from a single generating plant.

Although the exact compositions and layouts of substations vary, their equipment typically falls into the following categories:

- Circuit breakers;
- Disconnecting switches;
- Step-up and step-down transformers;
- Input and output T&D lines;
- Reactors, capacitors, and phase shifters;
- Electrical connections and insulators;
- Lightning arresters, static wires, and grounding systems;

- Automatic and manual protection equipment and housing;
- Telecommunications and remote control;
- Physical security; and
- Cyber security.

Circuit breakers are mechanical switching devices capable of carrying and breaking currents under normal operating conditions. They are also critical for protecting the system during abnormal system operating conditions, such as when short circuits occur in the system. Disconnecting switches are often used in conjunction with circuit breakers to provide added functionality and safety while system components are being maintained, repaired, or replaced.

High-voltage transformers (Figure 4) are often large (hundreds of tons), expensive (millions of dollars) devices that are difficult and time-consuming to replace. These boxlike devices are capable of transforming one type of line voltage into another. Transformers are used to step up (increase) or step down (decrease) voltages, thus providing an appropriate interface among generating units, transmission lines, and customer loads. The electrical capabilities and configurations of transformers vary. Replacing a transformer may take a long period because the inventory of spares is limited. On an emergency basis, deliveries from manufacturers may be made in less than a year.

Transmission lines (Figure 4) are the “transport highways” that move electricity from the generation sources to concentrated areas of customers. From there, the distribution system moves the electricity to the business or home where the customer uses it. Approximately 155,000 miles of AC transmission lines with voltages at 230 kV or higher were in place in 2002 in the United States, and about 43,000 miles in Canada.

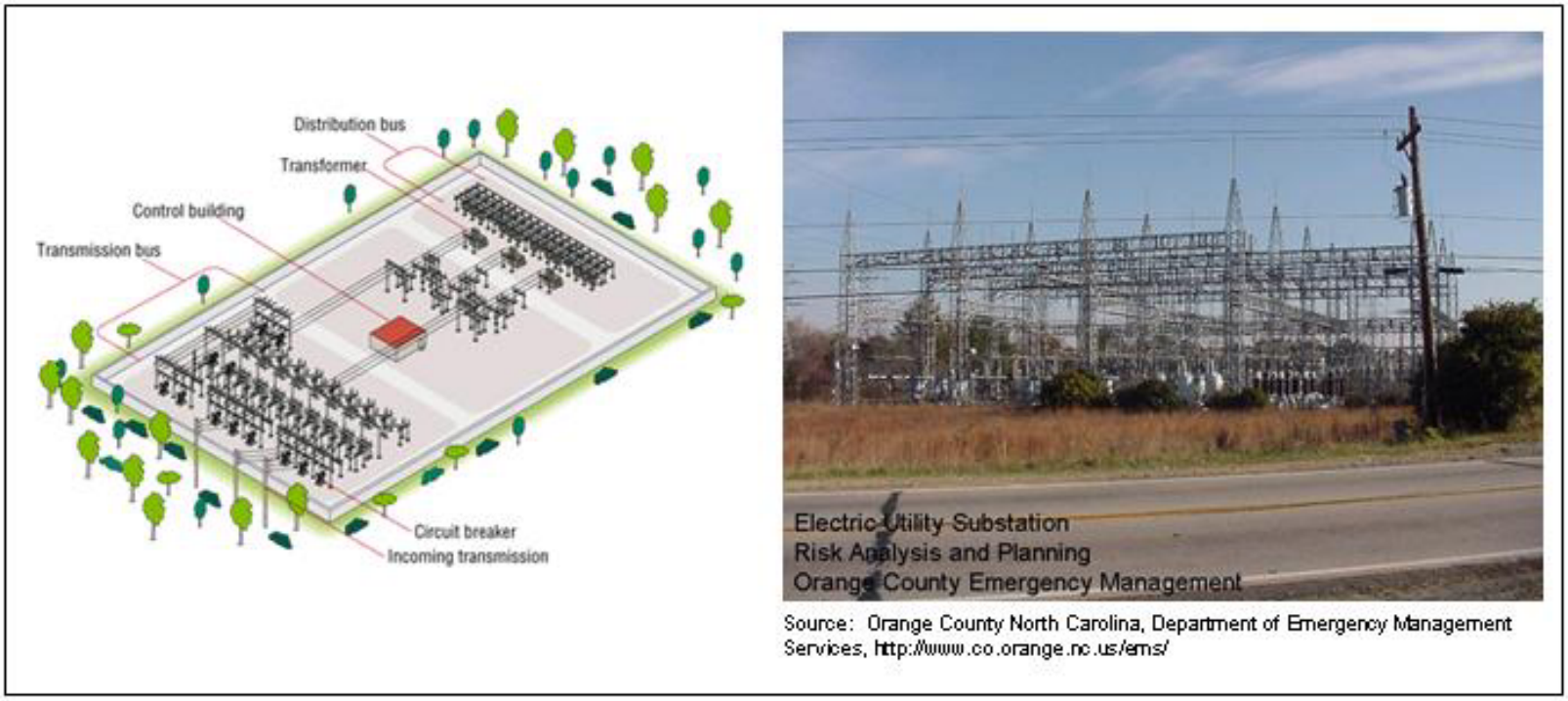


**Figure 3 General Layout of an Electric Power Substation**

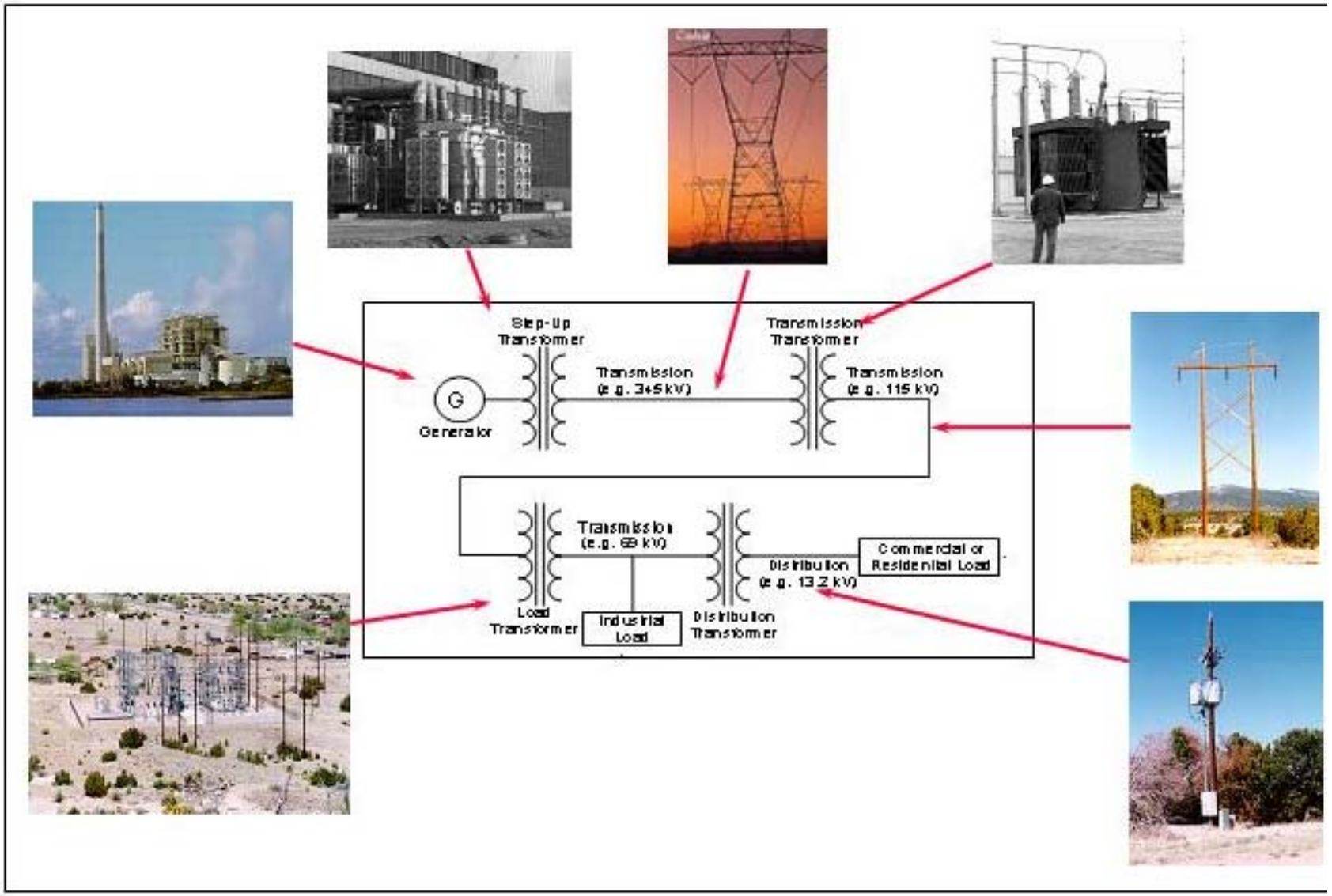


**Figure 4 Overview of Electric Power System Connectivity**

Reactors and capacitors are most often used to improve substation voltages, increase transmission line transfer capabilities, protect equipment from over-current or a transient voltage surge, and contribute to improvements in system reliability. Phase shifting transformers (phase shifters) are used to control or alter flows for various purposes, including reducing overloads, balancing flows during normal or outage conditions, and reducing losses.

The electrical connection and insulator arrangement can greatly affect the substation's reliability, cost, emergency operation, maintenance, repair, and safety. Various arrangements offer different tradeoffs with regard to these substation attributes, because the quantities and types of equipment are defined by the configuration of electrical connections. As a result, careful system design and modeling are important to appropriately define the optimal substation design. The adopted electrical equipment arrangement plays a critical role in a substation's overall vulnerability.

A substantial portion of substation design is devoted to the proper use of lightning arresters and an integrated static wire and grounding system. Together, these three items minimize the negative impacts to substation performance caused by lightning. In addition, the grounding system meets a critical design requirement for assuring proper equipment operation and a safe environment for maintenance personnel.

Events that can be triggered by either natural conditions or equipment failures are monitored and controlled by a network of automatic and manual protection equipment and controls. The protection equipment communicates information about events that can affect multiple substations in order to minimize the equipment damage that can result from such events. These actions can be controlled automatically through protective relaying equipment or manually through the supervisory control and data acquisition (SCADA) system. Substation control systems may include remote terminal units, programmable logic controllers, relays, telecommunications, uninterruptible power supplies, and battery backups.

Physical security at a substation typically includes fences or walls, gates, doors, and locks. Only a small percentage of substations have enhanced physical security that includes a badge access control system, door/gate contact alarms, perimeter intrusion detection, video surveillance, and vehicle barriers. A systems approach is advisable, in which detection, assessment, communications, and response are planned and supported by adequate policies, procedures, and resources. Substations are generally unattended.

Cyber security has become an increasingly important concern, because incidents affecting cyber systems that are critical to the reliability of electric systems have occurred and because the frequency and severity of cyber attacks are increasing. A basic cyber security program for electric system operations covers governance, planning, prevention, operations, incident response, and business continuity. The security effort focuses on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact electric system operations, and personnel.

The United States has approximately 63,000 substations. Most are AC substations, but a small number of direct-current (DC) substations serve as major system interconnections. These DC lines can be used to enhance system operations.

***Standards and Regulations***

There are numerous sources of information on public and private utilities. For example, additional substation statistics on all reporting utilities are available from Federal Energy Regulatory Commission Form 1, *Annual Report of Major Electric Utilities, Licensees and Others*, which represents a complete accounting of costs and revenues (including some equipment information) for utilities required to file the form. In particular, Form 1 contains information on substation voltage and capacity characterization, the number of substation transformers, and the number of spare transformers. The form also includes information as to whether the substation is classified as a transmission or distribution substation and whether the substation is attended or unattended by utility personnel. Thus, individuals interested in disrupting electrical systems can find out not only a substation's technical characteristics and inventories, but also whether it is attended. In recent years, utilities have had the option of declaring some of this information as "Privileged Treatment" and thus, not subject to public reporting.

In accordance with the Homeland Security Act of 2002, Section 214, the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate has prepared Critical Infrastructure Information (CII) procedures that are designed to protect important and sensitive information that the private sector voluntarily submits to the federal government to assist the nation in reducing the vulnerability of critical infrastructures to terrorist attack. These procedures are critical to ensuring that the nation is able to protect critical infrastructure, 85 percent of which is owned by the private sector.

The CII procedures will establish rules for receipt, care, and proper storage of the information and will ensure the Congressional mandate that such information not be shared with the general public. Subject to proper safeguards, this information will be used by the Department for the protection of critical infrastructure and to reduce the vulnerability of the infrastructure in the interest of national security.

Several organizations provide guidance, standards, and information for the electric sector. These include the North American Electric Reliability Council (NERC), Electricity Sector Information Sharing and Analysis Center (ESISAC), and Institute for Electrical and Electronics Engineers (IEEE). Brief descriptions of their related activities follow.

***North American Electric Reliability Council.*** NERC is a not-for-profit corporation whose members are 10 Regional Reliability Councils. The members of these councils come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; power marketers; and end-use customers. These entities account for virtually all the electricity supplied and used in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC operating and planning policies have been adopted over the years and are available at the NERC website. NERC recently prepared security guidelines for the electricity sector. The initial guidelines, which became effective on June 14, 2002, describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric

infrastructure systems. Additional guidelines have been adopted in 2003. The guidelines are advisory in nature.

The guidelines apply to "critical" operating assets. In the guidelines, a critical facility is defined as any facility or combination of facilities that, if severely damaged or destroyed, would have a significant impact on the ability to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

NERC also prepared a cyber security standard. This standard requires that responsible entities understand the role of cyber security in electric infrastructure reliability, identify their critical cyber assets related to bulk electric system operations, and have a security program in place. This program should mitigate the effect on bulk electric system operations from acts, either accidental or malicious, that could cause wide-ranging, harmful impacts. This standard is intended to ensure that appropriate mitigating plans and actions are in place, recognizing the differing roles of each responsible entity and the different risks being managed.

***Electricity Sector Information Sharing and Analysis Center.*** The ESISAC serves the electricity sector by facilitating communication among electricity sector participants, the federal government, and other critical infrastructure industries. It is the job of the ESISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, in order to help electricity sector participants take protective actions. The indications, analysis, and warnings (IAW) program is a set of guidelines for reporting operational and cyber incidents that adversely affect the electric power infrastructure. The IAW standard operating procedure (SOP) defines the criteria and thresholds for event reporting. The IAW program was developed in cooperation with the National Infrastructure Protection Center (NIPC, now part of the Department of Homeland Security).

***Institute for Electrical and Electronics Engineers.*** The IEEE maintains a large set of standards relevant to electric power substations. Included are standards on grounding, design, operation, and safety.

## TERRORIST ACTIVITY INDICATORS

### General Characteristics of Terrorist Surveillance

Terrorist surveillance may be fixed or mobile or both. 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; they may disguise themselves as street vendors, tourists, repair or delivery persons, 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 nonmobile facilities (i.e., driving past 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 in which 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 operations or in the 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 to loiter in these areas 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 high-dollar technological equipment.

Electronic surveillance, in this instance, refers to information gathering — legal and illegal — by terrorists using off-site computers. The type of data collected 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 (e.g., damage or modify) data or software. Equipment or process controls could also be affected (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 either be an end in itself or 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.

**Surveillance Indicators**

The surveillance indicators listed 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 on hand. For the most part, surveillance indicators refer to activities in the immediate vicinity of the electric power substation; 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 electric power substation, 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, although they may not be able to associate them with a specific critical asset because several critical assets may be located 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 electric power substation 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 | 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 calls, faxes, or mail concerning the facility, or key asset. |
| 7 | Nonfacility 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 to find personal information, maps, or other targeting examples. |
| 10 | Employees who change working behavior or work 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 airspace over infrastructure facilities; boat encroachment into restricted areas, especially if near critical infrastructure. |
| | (*Continued on next page.)* |

| Activities Observed or Reported | |
|---|---|
| 13 | A noted pattern or series of false alarms requiring a response by law enforcement or emergency services. |
| 14 | Theft of facility or contractor identification (ID) 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's 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 activity 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 at all times. |
| 25 | Arrest by local police of unknown persons. This activity would be more important if the facility or asset is located in a rural area rather than in or around a large city. |
| 26 | Traces of explosive or radioactive residue on facility vehicles during security checks by 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 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 nonfacility 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 by 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 targets (also applies to WMD). |
| 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**<br>*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 sale of large numbers of automatic or semi-automatic weapons. |
| 2 | Theft or sale of ammunition capable of being used in military weapons. |
| 3 | Reports of automatic (or unusual) weapons firing. |
| 4 | Seizures of modified weapons or equipment used to modify weapons (silencers, etc.). |
| 5 | Theft, loss, or sale of large-caliber sniper weapons .50 cal or larger. |
| 6 | Theft, sale, or reported seizure of night-vision equipment, in combination with other indicators. |
| 7 | Theft, sale, 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 | Theft or sale of large amounts of smokeless powder, blasting caps, or high-velocity explosives. |
| 5 | Sales of large amounts of high-nitrate fertilizer to nonagricultural purchasers or abnormally large amounts to agricultural purchasers.[1] |
| 6 | Large-scale theft or sale of combinations of ingredients for explosives (e.g., fuel oil, nitrates) beyond normal. |
| 7 | Theft or sale 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. |

[1] The Fertilizer Institute developed a "Know Your Customer" program following 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 indicator 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, 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 | Sale or theft of large quantities of baby formula (medium for biological agent growth) or an unexplained shortage of it. |
| 18 | Break-ins/tampering at water treatment or food processing/warehouse facilities. |
| 19 | Solicitation for sale 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 | Sale (to nonagricultural users) or theft 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 sale 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 WEBSITES

1. The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 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 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 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*, 2(3): 1–5, February 12, 2003 [http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf].

## USEFUL WEBSITES

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

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

3. Electric Sector Information Sharing and Analysis Center [http://www.esisac.com].

4. Institute of Electrical and Electronic Engineers; see, in particular, the substation standards [http://standards.ieee.org/catalog/olis/subst.html].

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

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

7. Federal Energy Regulatory Commission [http://www.ferc.gov/].

8. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October 1997 [http://www.ciao.gov/resource/pccip/report_index.htm].

9. Pansini, Anthony P., and Kenneth D. Smalling, *Basics of Electric Power Transmission,* PennWell Publishing Company, Tulsa, OK 1998.