POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: RAILROAD BRIDGES

Protective Security Division
Department of Homeland Security

Version 2, September 22, 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 railroad bridges, the most critical of which provide vital transportation links over rivers and other natural obstacles.

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. However, each observed anomaly or incident 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 infrastructure or asset of interest 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.

The geographic 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 and sometimes widely separated 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 the 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 leading 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.

RAILROAD BRIDGES BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to railroad bridges, it is useful to know how bridges are constructed and why these structures might be attractive targets for terrorist attack.

Terrorists may attack railroad bridges seeking to (1) endanger commuters or passengers or to harm the nearby population by damaging trains carrying hazardous or nuclear materials, (2) disrupt essential governmental shipments of military equipment by destroying trains or routes essential to that traffic, or (3) upset the United States (U.S.) economy by disrupting commercially essential shipments. Railroad bridges are vulnerable to attacks by explosives; tracks and switches are vulnerable to attacks by unbolting of joint bars or misalignment of switches; tunnels are vulnerable to attacks by explosives, chemical, or biological agents; and control/dispatching systems are vulnerable to explosive and information system attacks.

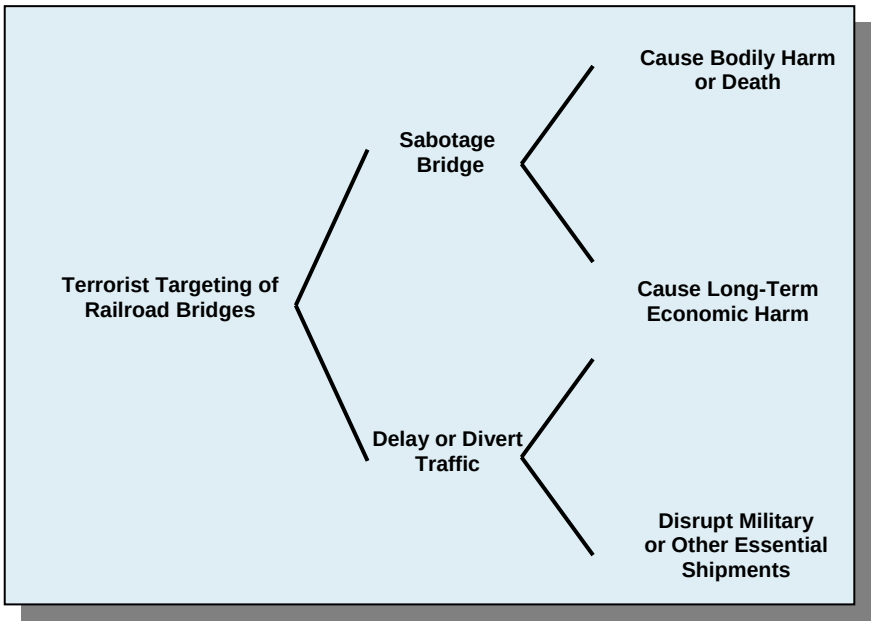

Figure 1 Terrorist Targeting Objectives for Railroad Bridges

Sector Description

Railroad bridges range from inspiring architectural marvels spanning giant bodies of water to tiny timber trestles offering passage over low spots on the prairie. Many railroad bridges in service today were built before World War I, and some are more than 100 years old.

All bridge designs, including railroad bridges, are comprised of four basic structural designs, with many variations within the structural design categories:

- Truss,
- Beam,
- Cantilever, and
- Arch.

***Truss Bridge*.** The truss bridge is very widely used for today's transportation needs, because it is strong and relatively inexpensive. It can be made of various materials, but steel and pre-stressed concrete are those most commonly used for its construction (like the beam bridge described below). The guiding principle behind the truss design is the use of triangles, which are very strong if used correctly. The greater amount of triangles a in a truss bridge, the greater the load the bridge can support. The structure of a truss, in fact, is usually combined with other structures to increase its strength.

Beam Bridge. The beam bridge has a very basic structure; it uses a beam resting on two or more piers. The weight of the load pushes down on the beam and is transferred to the piers, which determines its loading capacity. When a load pushes down on the beam, the beam's top edge is pushed together (compression), while the bottom edge is stretched (tension). Reinforced concrete is the ideal material for beam bridge construction, because the concrete efficiently withstands compressive forces, and the steel rods, imbedded within, resist the forces of tension.

The length of a beam bridge is limited, and for long spans, such bridges may require multiple piers. Therefore, the capacity of a beam bridge decreases with increasing span unless other reinforcing measures are included in the design. This does not mean beam bridges are not used to cross great distances; it only means that they must be daisy-chained together, creating a "continuous span." Most beam bridges, however, are extremely simple and span short distances.

***Cantilever Bridge*.** In a cantilever bridge, the beams are supported at only one end and carry a load at the other end, or distribute the load toward the center of the bridge. Long cantilevers are used in structures where clear space is required below, such as over a shipping channel or harbor.

***Arch Bridge*.** Arch bridges are one of the oldest types of bridges and have great natural strength. They rely on the concept that the arch displaces the weight from going straight down on the supports to having a portion of the force going straight down, the other portion being displaced diagonally to either side.

Since most railroad bridges are privately owned by various rail companies, there appears to be no complete and publicly available inventory of them. The *World Almanac and Book of Facts*, however, lists what it calls "notable" bridges, including railroad bridges, in North America. While the notable distinction is not defined, the characteristics of railroad bridges included in this source are reproduced in Table 1.

Table 1 "Notable" Railroad Bridges in the United States

No.	Bridge	Longest Span (ft.)	Year Opened	Location	Vehicular Traffic	Type of Construction
1	Hell Gate	1,038	1916	East River, New York		Arch (steel)
2	Baton Rouge	848	1940	Mississippi River		Cantilever
3	Vicksburg	825	1930	Mississippi River		Cantilever
4	Huey P Long	790	1935	New Orleans	Yes	Cantilever
5	Memphis (Harahan)	790	1916	Mississippi River		Cantilever
6	Memphis	790	1892	Mississippi River		Cantilever
7	Sciotoville, OH	775	1918	Ohio River		Truss (continuous)
8	Mingo Junction, WV	769	1904	Ohio River		Cantilever
9	Beaver, PA	767	1910	Ohio River		Cantilever
10	P&LE	750	1910	Beaver, PA		Cantilever
11	Metropolis	720	1917	Ohio River		Truss (simple)
12	Tanana River	700	1922	Nenana, AK		Truss (simple)
13	Cincinnati	675	1929	Ohio River		Truss (continuous)
14	Henderson	665	1933	Ohio River, IN-KY		Truss (simple)
15	Macarthur, IL-MO	647	1917	St. Louis, Mississippi R.	Yes	Truss (simple)
16	Castleton	598	1924	Hudson River		Truss (simple)
17	Arthur Kill	558	1959	NY-NJ		Draw Bridge Vertical Lift
18	Coos Bay	548	1914	Oregon		Draw Bridge Swing
19	Cape Cod Canal	544	1935	Massachusetts		Draw Bridge Vertical Lift
20	Cincinnati	542	1889	Ohio River		Truss (simple)
21	Delair, NJ	542	1960	Delaware River		Draw Bridge Vertical Lift
22	Martinez	528	1930	California		Truss (simple)
23	Fort Madison	525	1926	Mississippi River	Yes	Draw Bridge Swing
24	Willamette River	521	1908	Portland, OR		Draw Bridge Swing
25	East Omaha	519	1903	Missouri River		Draw Bridge Swing
26	McKinley, St. Louis	517	1910	Mississippi River	Yes	Truss (simple)
27	Duluth, MN	486	1897	St. Louis Bay		Draw Bridge Swing
28	C.M. & N. Railroad	474	1899	Chicago		Draw Bridge Swing
29	A-S-B Fratt	428	1912	Kansas City		Draw Bridge Vertical Lift
30	Harry S Truman	427	1945	Kansas City		Draw Bridge Vertical Lift
31	M-K-T Railroad	414	1932	Missouri River		Draw Bridge Vertical Lift
32	Cincinnati	365	1922	Ohio River		Draw Bridge Vertical Lift
33	Corpus Christi Harbor	344	1961	Corpus Christi, TX	Yes	Draw Bridge Vertical Lift
34	Martinez	328	1930	California		Draw Bridge Vertical Lift
35	Penn-Lehigh	322	1929	Newark Bay		Draw Bridge Vertical Lift
36	Chattanooga	310	1920	Tennessee River		Draw Bridge Vertical Lift

TERRORIST ACTIVITY INDICATORS

General Characteristics of Terrorist Surveillance

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 delivery persons, photographers, or even demonstrators.

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

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

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

Terrorists are also known to use advanced technology such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices, 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 the terrorists using offsite computers. This type of data gathering might include information such 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/traffic controls (e.g., damage a piece of equipment or open/close a switch to derail a train and cause a dangerous chemical release). Terrorists may also use technical means to intercept radio or telephone (including cell phone) traffic.

An electronic attack could be an end in itself or could be launched simultaneously with a physical attack. Thus, it is worthwhile to be aware of what information is being collected from

company and relevant government websites by offsite computer users and, if feasible, who is collecting this information. In addition, it is important to know whether attempts are being made to gain access to protected company computer systems and whether any attempts are successful.

Surveillance Indicators

The surveillance indicators in Exhibit 1 are examples of unusual activities that should be noted and considered as part of an overall 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 infrastructure or asset of interest. Most of the other indicator categories in this report address activities in a much larger region around the infrastructure or asset (e.g., 100 to 200 miles) that should be monitored.

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 infrastructure or asset but also those within a relatively large region around it. Local authorities should be aware of such activities. However, they may not be able to associate them with a specific critical asset, because there may be several 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 infrastructure or asset 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 it 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 offsite about practices pertaining to the facility, or an increase in personal e-mail, telephone, faxes, or mail concerning the facility or key asset.
7	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 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 offsite location to test the backup systems or recovery times of primary systems.
24	Increase in buildings being left unsecured or doors being left unlocked that are normally locked 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 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 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 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 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 *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.
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 armo, 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 offsite in suspicious locations or at unusual times.

*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 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, 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 nonagricultural 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.
31	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, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003 (http://www.whitehouse.gov/pcipb/physical.html).

2. *Terrorist Attack Indicators*, the html version of the file http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators.PDF (Reference site removed prior to publication.).

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 furtherance of WMD terrorist activities.

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

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

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

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

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

10. *The World's Longest Tunnel Page* (http://home.no.net/lotsberg/).

11. *William's Bridge Homepage* (http://www.jracademy.com/~wwedler/WilliamsBridgeHomepage.html).

12. *Bridges and Tunnels of Allegheny County and Pittsburgh* (http://www.pghbridges.com/index.htm).

13. Tompson, William C., Railroad Infrastructure Security, TRB Annual Meeting, January 14, 2002, Session 107 – Railroad Security (http://gulliver.trb.org/publications/am/presentations/Session107Thompson.pdf).

14. *The World Almanac and Book of Facts,* 1991, Pharos Books, New York, NY.

15. Association of American Railroads, *Class I Railroads* (http://www.aar.org/PubCommon/Documents/AboutTheIndustry/Statistics.pdf).

16. *Railroad Bridge and Trestle Pictures* (http://www.carrtracks.com/brdgndx.htm).

17. *Railway Track and Structures* (http://www.rtands.com/apr00/aging_bridges.html).

18. Needham High School, *A History of Bridges*, Needham, MA (http://www.needham.k12.ma.us/High_School/cur/sintros2/DE_KC/bridge.html).

19. Glendale Technology High School, *A General History of Bridges,* Glendale, NSW, Australia (http://www.glendaleh.schools.nsw.edu.au/faculty_pages/ind_arts_web/bridgeweb/bridge_general_history.htm).

20. Federal Emergency Management Agency, *HAZUS 99 User's Manual, Appendix C, Description of Lifeline Components* (http://www.fema.gov/hazus/).

21. Nagasaki University, *Geo-Environment Laboratory* (http://www.gel.civil.nagasaki-u.ac.jp/data/method.html). This site has descriptions of many types of tunneling equipment and techniques.

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. Federal Railroad Administration (http://www.fra.dot.gov/site/index.htm).
4. National Transportation Library (http://ntl.bts.gov/reference_shelf.cfm).
5. Bridge Picture File (http://www.welland.library.on.ca/digital/Bridpic.htm).
6. Transportation Research Board (http://www.trb.org/).