HOSPITALS

POTENTIAL INDICATORS OF TERRORIST ACTIVITY, COMMON VULNERABILITIES, AND PROTECTIVE MEASURES

Protective Security Coordination Division
Office of Infrastructure Protection
U.S. Department of Homeland Security

Version: October 5, 2007
Content: July 2007

WARNING

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid ‘need-to-know’ without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza, or locked area offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

For more information about this document, contact:
Protective Security Advisor Duty Desk (703-235-5724 or IPassessments@dhs.gov).
POTENTIAL INDICATORS OF TERRORIST ACTIVITY, COMMON VULNERABILITIES, AND PROTECTIVE MEASURES

Figure 1  A 700-Bed Hospital (Source: GWU 2006)

The American Hospital Association (AHA) reports that the United States had more than 5,700 hospitals with more than 37 million patient admissions in 2005. Approximately one-third of hospital care begins in the Emergency Department (ED). In 2004, there were 112.6 million ED visits.

This report presents the following information related to hospitals:

- Potential Indicators of Terrorist/Threat Activity
- Common Vulnerabilities
- Standards and Regulations
- Protective Measures
- Reference Material and Other Useful Information

This report is one of a series of documents that address how our nation can better protect its critical infrastructures and key resources. See contact on cover page for additional information.
HOSPITAL CHARACTERISTICS

The following sections provide a summary description of hospitals and their configurations and vulnerabilities that could be exploited by terrorists and other adversaries.

Characterization of the Industry

In 2005, the United States had 5,756 registered hospitals (i.e., those meeting criteria set by the American Hospital Association [AHA 2007a]), including profit and not-for-profit community hospitals (4,936), psychiatric hospitals (456), federal government hospitals (226), long-term care hospitals (118), and institutional hospitals (20). The hospitals collectively had 946,997 staffed beds and more than 37 million admissions during 2006. Rural hospitals generally maintain from 10 to 100 staffed beds, while larger, urban hospitals can have close to 1,000 staffed beds.

According to an annual evaluation conducted by U.S. News and World Report (2007), the five U.S. hospitals with top ratings in the most specialties were:

1. Johns Hopkins Hospital, Baltimore, MD;
2. Mayo Clinic, Rochester, MN;
3. UCLA Medical Center, Los Angeles, CA;
4. Cleveland Clinic, Cleveland, OH; and
5. Massachusetts General Hospital, Boston, MA.

Criteria used in the evaluation included mortality ratios, rankings by randomly selected board-certified physicians, numbers of procedures in a given specialty, and quality of nursing care and patient services.

The U.S. News and World Report evaluation does not include trauma services, which would be important in the event of a terrorist attack. Trauma centers are evaluated on the basis of criteria developed by the American College of Surgeons (2007). Level 1 trauma centers are prepared to care for the worst injuries, such as gunshot wounds and severed limbs; Level 2 centers are somewhat less well-equipped for these traumas, although still highly rated (Trauma.org 2007).

Professional organizations associated with hospital-based health care services are numerous. The AHA has a dual purpose as a trade organization and a public interest advocate. The AHA Web site [http://www.aha.org] provides an extensive list of other hospital and health-care-related organizations.

Full-service hospitals are vital to meeting the health care needs of the communities they serve. They provide a wide range of acute care and diagnostic services, support public health needs, and offer a myriad of other programs. While many of these roles also are performed by other health care providers, three are unique to hospitals (AHA 2007b):

- 24/7 access to care. The provision of health care services 24 hours a day, 7 days a week (24/7), 365 days a year;
• **Safety net role.** Caring for all patients who seek emergency care regardless of ability to pay;

• **Disaster readiness and response.** Ensuring that staff and facilities are prepared to care for victims of large-scale accidents, natural disasters, epidemics and terrorist actions.

### Common Facility Characteristics

Because the bed capacities and scale of services offered by hospitals vary widely, the types of buildings used as hospitals are also nonuniform (see Figures 2 and 3). Many rural hospital facilities are more than 30 years old because few federal resources have been devoted to
construction and renovation of rural hospitals since the Hill-Burton program ended in 1974 (Stensland et al. 2003). At the other end of the spectrum, newer urban hospitals are large and offer a wide range of services. At a minimum, all hospitals need to carry out the following functions: administration (including reception, admitting, and records), diagnosis and treatment, inpatient and outpatient areas, and support services (food service, engineering, and sanitation services).

The locations of these functions are generally arranged for ease of interaction and communication. For example, the diagnosis and treatment functions, including the radiology department, surgery, and laboratories, are often in the center of the facility, because both inpatient and outpatient areas rely on these functions. Inpatient and emergency services are generally separated from public reception and eating areas because of infection-control concerns and the need to meet patient privacy considerations. Inpatient nursing units are often organized to minimize the distance between nursing staff and patients (Carr 2004).

The hospital emergency (ER) department fulfills specialized functions. It needs to be easily accessible 24 hours per day and able to service critically ill and injured patients as well as patients with more routine or mild conditions. (The latter are increasingly using the ER for primary care because they lack health care insurance.) The ER commonly has a triage desk (for rapid evaluation and direction of patients to the appropriate caregiver). It is located close to hospital security services, has flexibility in room arrangement and use, and has a separate ventilation system from the rest of the hospital, with 100% fresh air supply and no recirculating air (Kliment et al. 2000). It often has a backup electrical system for critical-care equipment and monitoring, as well as one or more patient isolation rooms.

In times of disaster, communities look to hospitals not only to mobilize the resources to care for the ill and injured but also to provide food and shelter and coordinate relief and recovery efforts. To be ready, hospitals need (AHA 2007b):

- Comprehensive community disaster plans on which hospital and emergency workers have been trained and conducted exercises.

- Emergency apparatus that is well maintained (e.g., backup generators, communications systems, personal protective gear, decontamination units, stockpiled medical supplies).

- Surge capacity to meet the needs of large numbers of ill and injured patients.
POTENTIAL INDICATORS OF TERRORIST/THREAT ACTIVITY

Threats can be posed by an individual or a group that possesses the capability and intent to do harm. Domestic and international terrorists, adversarial nations, disaffected individuals or groups, disgruntled employees, and organized adversarial groups are all potential sources of threat. Threats can originate from individuals or groups with knowledge of the systems and equipment used at a facility. Insider information can be known by disgruntled or compromised employees, and detailed information on equipment and operating procedures can also be gathered from open sources or from active or former employees.

Threats Versus Hazards

Hazards and threats are two distinct entities. Hazards are situations or things that possess inherent and known danger. Empirical databases concerning hazards can exist or be created from historical records in order to determine the statistical probability of a future event. The effects of an incident involving a hazard can be forecast with relative precision because of the hazard’s known attributes. Security threats, however, are more difficult to characterize or quantify than routine hazards. The capabilities and intent of the purveyor of a threat may not be known, and the adaptive, thinking nature of the purveyor makes statistical analysis and calculations of probability a challenge.

The assessment of hazards falls within the discipline of safety, whereas the assessment of threats and the protection against them fall within the discipline of security. Often, the same group within an enterprise manages the responsibility for both sources of risk. Some safety and security efforts are mutually reinforcing; however, safety and security are not synonymous, and the two disciplines are different.

Targeting Objectives

To assess threats, one commonly accepted framework is to identify the threat purveyor’s objectives and goals, the potential targets, the means by which the threat might be carried out, and the knowledge and tactics required. A clear understanding of these factors, combined with an appreciation of the value of the assets and systems and the impact of unauthorized access and subsequent malicious activity, provides a basis for better defining the investment that might be needed to prevent such access. This process is useful for identifying realistic threats. Attackers have a range of objectives, as shown in Figure 4.
Weapons and Tactics

In targeting critical infrastructure, potential adversaries can employ a wide range of weapons, tools, and tactics, including the possible use of explosives. Some antagonists are gaining expertise in the use of less traditional methods, such as cyber attacks. Some weapons, tools, and tactics are discussed in the following sections.
Improvised Explosive Device

An improvised explosive device (IED), or ‘homemade bomb,’ can be constructed of commonly available materials, construction explosives (e.g., dynamite), or stolen military-grade explosives. An IED can be carried into a facility by an individual (e.g., a suicide bomber) or deposited in an unnoticed location for detonation by a timer or by remote control (Figure 5). Vehicle-borne IEDs (VBIEDs) are loaded into a car or truck or onto a motorcycle. These vehicles can be parked close to the facility and placed where large numbers of people gather, or they can be crashed through barriers and then detonated. They are much larger and more dangerous than IEDs carried by an individual. VBIEDs are very common throughout the world.

Arson

Intentional fires can be set by tossing highly flammable materials (such as gasoline) into a facility (see Figure 6). Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson is a threat before, during, and after normal business hours.
Small Arms Attack

Conventional firearms, automatic weapons, shoulder-carried rocket-propelled grenades, or similar weapons can be used to indiscriminately shoot people or take hostages (Figure 7).

Figure 7  Small Arms Attack (Left to Right): Terrorists with Conventional Small Firearms and Grenade Launchers

Assassination/Kidnapping

Many terrorist acts have involved the assassination of key personnel or the kidnapping of individuals and taking of hostages (Figure 8).

Figure 8  Various Hostage and Kidnapping Situations

Chemical Attack

Chemicals can be exploited or used by terrorists as a weapon. Such chemicals include toxic industrial chemicals (e.g., ammonia, hydrogen fluoride) already present at the site either as part of a manufacturing process or for use in normal operations (e.g., chlorine stored on site for use in water treatment plants, swimming pools) or chemicals transported by truck or railroad and brought near a facility or large gathering of people, where they could be dispersed by explosives (Figure 9). Chemical warfare agents (e.g., sarin, VX) are another weapon of concern. Although not readily available, they have been procured and used by terrorists. The 1995 sarin gas attack in the Tokyo subway is an example.
Biological Attack

Biological pathogens (e.g., anthrax, botulin, plague) can cause disease and are attractive to terrorists because of their potential to cause mass casualties and exhaust response resources. Biological agents can be dispersed in the atmosphere (e.g., via crop-dusting aircraft); introduced into a facility through its heating, ventilation, and air-conditioning (HVAC) system; or spread by contact (e.g., through contaminated letters delivered by mail) (Figure 10).

Nuclear/Radiological Attack

Weapons-grade nuclear material is relatively difficult to obtain. However, some sources of nuclear and radiological material are more readily available (e.g., from medical diagnostic equipment) and are more easily delivered. Radiological agents include radioactive material from various sources, such as medical or industrial equipment (Figure 11). All of these agents could be introduced into a facility either directly (e.g., by spreading them on surfaces where people will have direct contact) or through the HVAC system. Radiological dispersion devices (RDDs), often called ‘dirty bombs,’ have these materials attached to an explosive to create a wide area of contamination.
Sabotage

The disruption or damage to or destruction of a structure or facility through sabotage (Figure 12), the introduction of hazardous materials (HAZMAT) into the facility, and the contamination of facility products are of concern. Sabotage can be perpetrated by employees or by outsiders. In some cases, sabotage is designed to release HAZMAT from a facility into the surrounding area or to cause cascading problems across interdependent critical infrastructures.

Aircraft Attack

Both commercial and general aviation aircraft can be hijacked and used to deliver attackers, explosives, or HAZMAT to an area or facility. The aircraft themselves can also be used as weapons (Figure 13).
Maritime Attack

Ships and boats of various sizes or cargo containers can be used to deliver attackers, explosives, or HAZMAT to an area or facility (Figure 14). The vessels themselves can be used as weapons when outfitted as waterborne IEDs (WBIEDs) and maneuvered into position near a target or rammed into a target. Targets include ships, ports, and bridges. The attack on the USS Cole is an example of a maritime attack.

Cyber Attack

Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Information can be altered, corrupted to render it unusable, or stolen. Information systems can be attacked with the intent of overloading the equipment (e.g., denial-of-service attacks). Some information systems can be used to mount attacks on other systems. Supervisory control and data acquisition (SCADA) and other process control systems that are used to control mechanical equipment (e.g., pipelines, railroad switches, industrial process streams) can be infiltrated so that the equipment can be operated in such a way as to cause damage and inflict on-site and off-site casualties (Figure 15).
Al-Qaeda’s Surveillance Objectives

The list of surveillance objectives provided in the next chart is from captured reports on how to ‘case’ target subjects that were developed by al-Qaeda operatives to be used against the U.S. financial sector. While similar reports targeting assets in other sectors have not been recovered to date, the tactics are fairly uniform, and studying the list can help asset owners recognize potential surveillance activities.

Understanding the signature behaviors associated with terrorist operational planning will help infrastructure security personnel better portray real and perceived terrorist surveillance efforts in their reports on suspicious incidents. Improved reports and documentation could ultimately lead to the disruption of terrorist attack planning. While much is unknown about the terrorist threat to the nation, it is known that al-Qaeda and its affiliates remain interested in striking the United States.
### SURVEILLANCE OBJECTIVES

These objectives describe the kinds of information that terrorists monitor when planning an attack.

<table>
<thead>
<tr>
<th><strong>Surveillance and Countersurveillance</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Identity of places where further surveillance can take place</td>
</tr>
<tr>
<td>- Identity of places where countersurveillance can be detected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Facility Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Presence or absence of security cameras</td>
</tr>
<tr>
<td>- Number, location, type, and coverage of security cameras</td>
</tr>
<tr>
<td>- Security screening procedures for employees, visitors, and vehicles</td>
</tr>
<tr>
<td>- Procedures for changing of the guard</td>
</tr>
<tr>
<td>- Opportunities for theft of facility identification (ID) cards or special license plates</td>
</tr>
<tr>
<td>- Proximity to first-responder locations</td>
</tr>
<tr>
<td>- Security event response times</td>
</tr>
<tr>
<td>- Number, gender, ethnicity, location, dress, weapons, and equipment of security/police forces</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Facility Access</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Configuration and staffing of control points</td>
</tr>
<tr>
<td>- Visitor access procedures to restricted areas</td>
</tr>
<tr>
<td>- Availability of tours</td>
</tr>
<tr>
<td>- Location of roadways, entrances, parking lots, gates, and access points</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Facility Construction</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Construction materials used</td>
</tr>
<tr>
<td>- Building shape, height, and setbacks</td>
</tr>
<tr>
<td>- Location of vulnerable structural components</td>
</tr>
<tr>
<td>- Opportunities for cascading damage effects</td>
</tr>
<tr>
<td>- Location of executive offices and employee meeting places</td>
</tr>
<tr>
<td>- Location of power and HVAC systems</td>
</tr>
<tr>
<td>- Adequacy of emergency exits, escape routes, and fire suppression systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Target Dynamics</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Shift changes</td>
</tr>
<tr>
<td>- Patterns of concentration of people and vehicles; traffic congestion</td>
</tr>
<tr>
<td>- Nearby people and vehicle movement throughout the day</td>
</tr>
<tr>
<td>- Monitoring of police radio frequencies and recording of emergency response times</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Secondary Targets</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Nearby alternative targets</td>
</tr>
<tr>
<td>- Nearby collateral targets</td>
</tr>
</tbody>
</table>
Potential Indicators

An indicator could be any suspicious activity that warrants a reaction. A reaction could be an investigation, a root-cause analysis, a communication, or an emergency response.

When people look at the normal environment, the unusual should attract their attention. If individuals know their environment, they will more readily notice something out of the ordinary or something that does not quite ‘fit.’ The same idea applies to the threat environment. People operate and inspect facilities and purchase, store, or use industrial products every day. Constant attention to these indicators can help people know when to alert officials of the possibility of an incident.

The section below on imminent attack indicators is followed by sections that describe surveillance indicators; transactional and behavioral indicators; and indicators of possible threats from weapons, explosives, or chemical, biological, or radiological (CBR) materials and devices. The charts in these sections outline additional indicators of possible surveillance activity or focus. These charts are fairly detailed; however, their main intent is to give asset owners and employees information about surveillance activities that might be associated with a given asset and to help them recognize (and then report) any unusual events.

Imminent Attack Indicators

Indicators of an imminent attack include people who demonstrate unusual or suspicious behavior, vehicles that demonstrate unusual or suspicious behavior, or unusual or suspicious packages that require an immediate response. Included in this category are practice-run indicators (i.e., activities associated with rehearsing or carrying out exercises for a terrorist attack).
### IMMINENT ATTACK INDICATORS (at or near a facility)

*These indicators suggest unusual and suspicious behavior that requires immediate response.*

<table>
<thead>
<tr>
<th>Indicators about Activities (Observed or Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Persons in crowded areas wearing unusually bulky clothing that might conceal explosives who could be</td>
</tr>
<tr>
<td>- Patting down or feeling under their clothing or concealing weapons</td>
</tr>
<tr>
<td>- Showing electrical wires from under their clothing or tightly clutching an object that could be a trigger device</td>
</tr>
<tr>
<td>- Displaying excessive nervousness or anxiety</td>
</tr>
<tr>
<td>- Wearing excessive amounts of cologne or perfume to mask the scent of explosives</td>
</tr>
<tr>
<td>• Persons or teams of people attempting to gain illegal entry (e.g., scaling fences, breaking into doors) or appearing to prepare to launch standoff weapons (e.g., rocket-propelled grenades) at the facility</td>
</tr>
<tr>
<td>• Nonmilitary persons seen with military-style weapons and clothing or equipment</td>
</tr>
<tr>
<td>• Any type of vehicle illegally located near facility buildings or places with large numbers of people (The vehicle may be unattended or may have a driver [e.g., who could detonate explosives]. A driver may [a] demonstrate nervousness or anxiety, [b] be constantly scanning the area for law enforcement personnel, or [c] be looking for ways to impact the largest number of victims.)</td>
</tr>
<tr>
<td>• Unexpected or unfamiliar delivery trucks arriving at the facility</td>
</tr>
<tr>
<td>• Vehicles (a) approaching at an unusually high speed or (b) steering around barriers and traffic controls</td>
</tr>
<tr>
<td>• Unattended package (e.g., backpack, briefcase, box) that might contain explosives</td>
</tr>
<tr>
<td>• Suspicious package and/or letter received by mail that might contain explosives or CBR agents (The packages or mail may have (a) no return address, (b) excessive postage, (c) been sent from outside the United States, (d) indications of leaking liquids, or (e) unusual odors.)</td>
</tr>
<tr>
<td>• Evidence of unauthorized access to HVAC areas of a building (Indications of unusual substances, such as unknown powders, droplets, or mists, may be present near air intakes.)</td>
</tr>
<tr>
<td>• Recent damage to a perimeter fence or gate or damage to perimeter lighting, cameras, or sensors</td>
</tr>
</tbody>
</table>

### Practice-Run Indicators (Observed or Reported)

<table>
<thead>
<tr>
<th>Practice-Run Indicators (Observed or Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Persons with an unusual interest in security measures, personnel, entry points, access controls, or barriers</td>
</tr>
<tr>
<td>• Unusual behavior, such as people staring or quickly looking away or vehicles entering or leaving parking areas</td>
</tr>
<tr>
<td>• Training scenarios carried out by paramilitary groups or other organizations advocating violence</td>
</tr>
<tr>
<td>• Persons displaying anxiety, such as retracing their steps</td>
</tr>
<tr>
<td>• Persons observing security drills or procedures</td>
</tr>
<tr>
<td>• Persons mapping routes or timing traffic lights and traffic flow</td>
</tr>
<tr>
<td>• Persons questioning security or facility personnel</td>
</tr>
<tr>
<td>• Persons wearing disguises to elude detection or gain access to restricted areas (including wearing military, medical, firefighter, or police uniforms or dressing like a pregnant woman)</td>
</tr>
</tbody>
</table>
Surveillance Indicators

Surveillance indicators are persons or unusual activities in the vicinity of a critical infrastructure or key resource that are intended to gather information about the asset and/or its operations, shipments, or protective measures.

Terrorist surveillance may be fixed or mobile. Fixed surveillance is performed from a static, often concealed position, possibly an adjacent building, business, other facility, or high ground. 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, to provide a plausible reason for being in the area.

Mobile surveillance usually entails observing and following key vehicles or human targets, although it can be conducted against nonmobile facilities (i.e., drive-by site observations).

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. Public gathering areas provide convenient venues for 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 (GPSs). It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance refers to information gathering, legal and illegal, by terrorists using off-site computers or other technology. The type of data gathered may include critical asset information, security procedures, or system passwords. Terrorists may use an array of technical means to intercept e-mail, radio, cell phone, and pager traffic.

In addition, terrorists may launch an electronic attack that could affect databases, networks, software, or control systems. Such attacks may be intended to cause direct damage (e.g., delete data records), modify the response of a system (e.g., open a process valve when a command would normally close a process valve), or steal information (e.g., credit card data). An electronic attack could also serve as a preemptive strike intended to create confusion while simultaneously launching a physical attack.

The surveillance indicators listed in the following chart are examples of unusual activities that should be noted, with consideration given to the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other experience.
<table>
<thead>
<tr>
<th><strong>SURVEILLANCE INDICATORS</strong> (at or near a facility)</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>These indicators suggest information gathering activities may be under way.</em></td>
</tr>
</tbody>
</table>

### Indicators about People (Observed or Reported)

- Frequent or unusual use or possession of video, camera, recording, or observation equipment
- Possession of installation photos or diagrams with highlighted areas or notes regarding infrastructure
- Possession or observed use of night-vision devices
- Persons parking, standing, or loitering in the same area over multiple days with no reasonable explanation for doing so
- Persons questioning staff off-site about facility practices, or an increase in the amount of inquiries about critical features
- Persons not associated with the facility showing an increased interest in the surrounding area
- Staff willfully associating with suspicious individuals
- Computer hackers attempting to access sites for personal information, maps, or other targeting data
- An employee whose working behavior undergoes an unusual change or who begins to work irregular hours
- Persons showing an unusual interest in receipts or deliveries, especially of HAZMAT
- Unfamiliar cleaning/contract crews with passable credentials; attempts to access unauthorized areas
- Arrest of unknown persons by local police (may be more important if facility is located in a rural area)

### Indicators about Activities (Observed or Reported)

- Downloading of materials (e.g., maps, schematics) useful in surveillance or attack-planning activities
- Repeated attempts to access protected computer information from the same organization or country
- Successful penetration and access of protected computer systems with critical information
- Attempts to obtain information about the facility (e.g., building blueprints from public sources)
- Aircraft flyover or boat encroachment into restricted areas
- An abandoned or illegally parked vehicle in the area of a key facility or employee/patient gathering area
- Increased interest in outside components (e.g., electrical equipment) that is less protected or not protected at all
- Unexplained power outages that may be intentionally testing emergency response or recovery plans
- An increase in threats that may be intentionally testing emergency response or recovery plans
- A noted pattern of false alarms requiring a response by law enforcement or emergency services personnel
- Unexplained increase in the number of incidences in which security and safety devices are left unsecured or in unsafe conditions
- Theft of ID cards or uniforms, or possession of such items by unauthorized persons
- An increase in violations of standard operating procedures by security guards at key posts
- Sudden loss or theft of guard force communications equipment, keys, or access cards
- Recent damage to fences or gates or to perimeter lighting, cameras, or sensor devices
- Indications or observations of persons collecting or searching through trash
- Displaced or misaligned manhole covers or open service access doors near critical sites
- Unusual maintenance activities near the facility (e.g., out-of-season road repairs)
Transactional and Behavioral Indicators

Transactional and behavioral indicators are suspicious purchases or sales of materials that could be used in an act of terrorism or criminal activity. They may involve vendors or suppliers, staff, or persons with knowledge of terrorist incidents or crimes in the vicinity of a facility.

Transactional indicators are unusual, atypical, or incomplete procedures or events associated with an inquiry about equipment and materials or an attempted purchase or sale of these items.

Behavioral indicators are actions or inactions on the part of a customer, vendor, supplier, or staff member that are inconsistent with normal behavioral patterns.

<table>
<thead>
<tr>
<th>TRANSACTIONAL AND BEHAVIORALINDICATORS (at or near a facility)</th>
</tr>
</thead>
<tbody>
<tr>
<td>These are indicators of atypical procedures or actions by customers, vendors, or suppliers.</td>
</tr>
</tbody>
</table>

**Transactional Indicators**
- Approach from a previously unknown vendor, supplier, or customer whose identity is not clear
- Transaction involving an intermediary agent or consignee that is atypical in light of usual business
- An agent or customer associated with a military-related business, such as foreign armed forces
- Unusual request concerning the shipment or labeling of goods
- Packaging that is inconsistent with the shipping mode
- Request for excessive confidentiality regarding a purchase, sale, or delivery
- Orders for excessive quantities of personal safety/security devices that are outside normal needs
- Requests for normally unnecessary devices/supplies coupled with an unconvincing explanation for the need
- Vendor, supplier, or customer that uses a different name for different transactions
- Orders for excessive quantities of personal safety/security devices that are outside normal needs
- Requests for normally unnecessary devices/supplies coupled with an unconvincing explanation for the need
- Equipment, chemicals, or materials stolen or ‘lost’ during shipment or shortly after delivery

**Behavioral Indicators**
- Delivery that is unexpected, out of the norm, without explanation, or associated with suspicious paperwork
- Excessive request for site access by delivery person or delivery vehicle
- Evasive responses or reluctance to give sufficient explanations for use or purpose of materials
- Reluctance to provide location data, such as business address, delivery point, or shipping origin
- Reluctance to provide clear answers to routine commercial or technical questions
- Reason given for purchase or sale does not match the usual business or technological level
- No offer of, request for, or refusal of technical assistance when such action is generally standard
- Equipment or material is said to be for a use that is inconsistent with its design or normal purpose
- Theft of equipment or material that has no practical use outside a legitimate business practice
- Apparent lack of familiarity with the ‘business’ or its nomenclature or a lack of knowledge of how transactions of this type are handled
- Inconsistency of information that is provided (e.g., phone number or address) with what is known
Weapons, Explosives, and Chemical, Biological, or Radiological Indicators

Suspicious activities involving threats from weapons, explosives, or CBR materials may also warrant reactions such as an investigation, a communication, or an emergency response.

Weapons

Indicators of possible use of weapons against a facility include the purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out an intended action. Items of interest include not only guns, automatic weapons, and rifles, but also ammunition and equipment, such as night-vision goggles and body armor, and relevant training exercises and classes. The following chart expands on this description of weapons indicators.

<table>
<thead>
<tr>
<th>WEAPONS INDICATORS (at or near a facility)</th>
</tr>
</thead>
<tbody>
<tr>
<td>These indicators provide insights into the use or planned use of weapons.</td>
</tr>
</tbody>
</table>

**Indicators about Activities (Observed or Reported)**
- Reports of automatic or unusual weapons firing
- People wearing clothing that is not consistent with the local weather
- Training scenarios carried out by paramilitary groups or other organizations advocating violence
- Theft, transactions, or seizures of large numbers of
  - Automatic or semiautomatic weapons
  - Ammunition capable of being used in military weapons or modified weapons
  - Equipment used to modify weapons (e.g., silencers)
  - Large-caliber sniper weapons
  - Night-vision equipment
  - Body armor, especially in combination with other indicators

Explosives

Indicators of explosive or incendiary materials and devices that could be used by terrorists include the production, purchase, theft, testing, or storage of any kind of these materials. The next chart describes indicators of those activities in addition to indicators of VBIEDs.

VBIEDs are dangerous because they are inherently mobile and inconspicuous by design, yet they can conceal large amounts of explosives and therefore do not always have to penetrate perimeter security defenses to be effective. The VBIED indicators listed in this next chart are taken from lessons learned in Iraq.
EXPLOSIVE AND INCENDIARY INDICATORS (at or near a facility)
These indicators provide insight into the presence of explosives or explosive devices.

<table>
<thead>
<tr>
<th>Indicators about People (Observed or Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Persons stopped or observed with unexplained amounts of explosives</td>
</tr>
<tr>
<td>• Unidentified persons making inappropriate inquiries about explosives or their construction</td>
</tr>
<tr>
<td>• Treated or untreated chemical burns or missing hands and/or fingers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indicators about Activities (Observed or Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Thefts, transactions, or seizures of large amounts of smokeless powder, blasting caps, high-velocity explosives, sensitive chemicals, combinations of ingredients for explosives (e.g., fuel oil, high-nitrate fertilizer), containers (e.g., propane bottles), or vehicles (e.g., trucks) that result or could result in IEDs, especially in combination with other indicators</td>
</tr>
<tr>
<td>• Modification of a sedan, van, delivery truck, water or concrete truck, or semitrailer to carry explosives</td>
</tr>
<tr>
<td>• Traces of explosive residue on visitor or delivery vehicles during explosive detection checks</td>
</tr>
<tr>
<td>• Unexpected or unfamiliar delivery trucks or deliveries</td>
</tr>
<tr>
<td>• Delivery of chemicals or suspicious materials to rental or self-storage units or out-buildings</td>
</tr>
<tr>
<td>• Vehicles containing unusual or suspicious parcels or materials</td>
</tr>
<tr>
<td>• Suspicious packages (e.g., unexpected deliveries, return-address errors, or excessive postage)</td>
</tr>
<tr>
<td>• Unattended packages, briefcases, or other containers</td>
</tr>
<tr>
<td>• Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in storage out-buildings, nearby homes, apartments, hotel rooms, or self-storage units</td>
</tr>
<tr>
<td>• Reports of explosions, particularly in rural or wooded areas</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indicators about VBIEDs (Observed or Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Noticeable sagging of the vehicle on its springs, caused by the heavy weight of explosives (Ordinarily, explosives are placed toward the rear of the vehicle, causing it to ride lower in the rear. However, commercial trucks carrying VBIEDs are designed to carry the weight and may not appear to sag.)</td>
</tr>
<tr>
<td>• Darkened or covered windows to conceal either the vehicle’s contents or the driver’s actions</td>
</tr>
<tr>
<td>• Unusual vehicle items, such as gas cylinders, wires, leaflets, large bags or boxes, or extra batteries</td>
</tr>
<tr>
<td>• Indications of a triggering device (e.g., a switch, radio transmitter, timer, wires, or ropes passing from the front seat to the rear of the vehicle) visible near the driver, under the seat, or within arm’s reach</td>
</tr>
<tr>
<td>• Additional fuel tanks, used to hide explosives or to provide additional gasoline to fuel an explosion</td>
</tr>
<tr>
<td>• Holes made in the vehicle body to hide explosives and then crudely covered</td>
</tr>
<tr>
<td>• Evidence that an interior door panel has been removed to hide explosives</td>
</tr>
<tr>
<td>• Recent painting of the vehicle to cover body alterations</td>
</tr>
<tr>
<td>• Any disturbance to the undercoating or dirt on the bottom of a vehicle</td>
</tr>
<tr>
<td>• Additional antennas on the vehicle for radio-controlled devices</td>
</tr>
<tr>
<td>• Unusual smells, such as a burning time fuse, gasoline, or fertilizer</td>
</tr>
<tr>
<td>• Presence of powder or prills (e.g., small rounded granular material) left when explosives are loaded</td>
</tr>
<tr>
<td>• Presence of a vehicle in an area where it should not be, perhaps parked illegally or at an unusual time</td>
</tr>
</tbody>
</table>
Chemical, Biological, and Radioactive (CBR) Materials

Chemical agents, biological species, and hazardous radioactive materials could also be threats to infrastructures, populations, and agriculture. Indicators of the possible presence of those materials are related to their production, purchase, theft, testing, or storage and are described in the next chart.

**CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL (CBR) INDICATORS (at or near a facility)**

These indicators provide insights into the presence of CBR materials.

<table>
<thead>
<tr>
<th>Equipment Configuration Indicators (Observed or Reported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Thefts, transactions, or seizures of sophisticated personal protective equipment (PPE), such as ‘A’ level Tyvek, self-contained breathing apparatus (SCBA), or sophisticated filtering, air-scrubbing, or containment equipment</td>
</tr>
<tr>
<td>- An area under strict security control that is inconsistent or out of character with normal operations</td>
</tr>
<tr>
<td>- Suspicious packages (e.g., unexpected deliveries, return-address errors, or excessive postage)</td>
</tr>
<tr>
<td>- Unattended packages, briefcases, or other containers</td>
</tr>
<tr>
<td>- Unexpected or unfamiliar delivery trucks or deliveries</td>
</tr>
<tr>
<td>- Vehicles containing unusual or suspicious parcels or materials</td>
</tr>
</tbody>
</table>

**Chemical Agent Indicators (Observed or Reported)**

- Thefts, transactions, or seizures of explosives or restricted or sensitive chemicals
- Inappropriate inquiries regarding chemical usage, transactions, storage, or transportation
- Delivery of chemicals or suspicious materials to rental or self-storage units or out-buildings
- Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in storage out-buildings, nearby homes, apartments, hotel rooms, or self-storage units
- Treated or untreated chemical burns or missing hands and/or fingers
- Unusual containers, powders, droplets, or mist clouds near HVAC equipment or air-intake systems

**Biological Agent Indicators (Observed or Reported)**

- Thefts, transactions, or seizures of large quantities of baby formula (a medium used for growing biological agents), live and/or lethal amounts of agents/toxins/diseases (from medical supply companies or labs), or dispensing systems, such as agricultural sprayers or crop-dusting aircraft or foggers (especially to nonagricultural users)
- Inappropriate inquiries regarding biological agent usage, storage, or transportation
- A break-in at or tampering with a nearby water treatment facility or food processing/warehouse facility
- Multiple, unexplained human or animal illnesses (or deaths), especially illnesses not native to area
- Unusual containers, powders, droplets, or mist clouds near HVAC equipment or air-intake systems

**Radioactive Material Indicators (Observed or Reported)**

- Thefts, transactions, or seizures of radioactive materials from medical supply companies or labs
- Inappropriate inquiries regarding radiological material usage, storage, or transportation
- A break-in at or tampering with facilities that store radioactive materials or radioactive wastes
- Multiple, unexplained human or animal radiation burns or radiation sickness or radiation deaths
COMMON VULNERABILITIES

Key Vulnerabilities

The following is a list of the key common vulnerabilities of hospitals. In addition, a number of general vulnerabilities that exist at many different infrastructure segments may also apply to hospitals.

Visibility, Accessibility, and Population

- **Open to public with multiple entrances.** Many hospitals are easily accessible to individuals who may be adversaries with malicious intent. The main entrance at most hospitals generally has an information desk and may or may not have a security presence. More stringent security measures such as metal detectors are rarely present. The availability of side entrances away from the main entrance can allow an adversary access without attracting the attention of hospital staff or security. Large hospitals may have 20 to 50 unsecured entrances. Some hospitals are decreasing the number of entrances as they conduct renovations (Kliment et al. 2000).

- **Easy access by motorized vehicles, including parking close to or under the hospital.** Hospitals must be easily accessible to ambulances and other vehicles transporting individuals who are not ambulatory. Furthermore, for patient and visitor convenience, the parking facilities must be close to the hospital. Because the potential for damage is so great if a bomb detonates in a vehicle beneath the facility, underground parking facilities are a substantial hazard. Outdoor ambulance entrances and walk-up entrances can be somewhat protected through measures such as landscape features and barriers to reduce blast-wave propagation (Pietrzak 2004).

- **Potential for mass casualties.** If hospitals are attacked, there is the potential for a large number of casualties because of their proximity to highly populated and traveled areas, along with their normal traffic of hospital staffing, patients, and visitors.

- **Diverse staff/lack of background checks.** Hospitals require a large, diverse workforce, and background checks may not be conducted for all workers, particularly housekeeping, food service, or facility maintenance workers. Lack of background checks may be a particular problem with respect to contract workers. Many hospitals provide opportunities for teaching and research to numerous visiting professionals, including students, interns, residents, and scientists. Some hospitals are tailored to provide care to noncitizens.
Presence of Hazardous, Toxic, and Explosive Materials

- Potential to spread dangerous chemicals, microbes, or radionuclides through the ventilation system. This vulnerability is common to all large buildings. Many hospitals have taken steps to partially mitigate this hazard through the use of both HEPA filters and ultraviolet germicidal irradiation filters in their ventilation systems (FEMA 2003). HEPA filters are 99.97% efficient in capturing particulate matter greater than 0.3 micrometer in diameter (including bacterial spores), while ultraviolet (UV) germicidal irradiation kills all viruses and most bacteria. Filtration in hospital ventilation systems would also be somewhat efficient in limiting radiation exposures because radionuclides are generally found in the form of micrometer-sized aerosols. However, if radionuclides were dispersed in a ventilation system, the system would require decontamination. Neither HEPA filtration nor UV radiation would limit distribution of chemical agents, which are generally gases or vapors. Chemically treated activated carbon filters are currently recommended by the U.S. Department of Defense for collecting chemical warfare agents (FEMA 2003). Such sorbent filters are not in wide use in ventilation systems because they are technically difficult to maintain and because efficiencies may not be adequate to be protective. Air intakes in high, inaccessible areas are less vulnerable to the intentional introduction of hazardous materials. Outdoor air intakes in low, accessible areas can be made less vulnerable by enclosures. The Association for Professionals in Infection Control and Epidemiology recommends physically inaccessible outdoor air intakes for health-care facilities (APIC 2004).

- Potential for explosions and fire, such as liquid fuel or gases or medical gases. These substances, which are routinely present at hospitals, could be tampered with to cause an explosion or fire. Significant quantities may or may not be kept in secured areas (e.g., fenced areas, concealed areas).

- Attractive theft targets, such as radionuclides and pharmaceuticals. These substances would most likely be the targets of theft. Radionuclides released to a hospital ventilation system could result in evacuation and costly cleanup activities.

- Unprotected, easily accessible utility supplies. Gas lines, fuel tanks, electric power transformers, generators, oxygen tanks, and water lines may all be located in or feed to the facility from a single point of entry. These structures and components may be in easily accessed areas, in open view of the public, and unprotected.
Previous Incidents

The following is a list of incidents that have occurred at hospitals that illustrate some of the vulnerabilities.

- In February 2007, seven NATO troops were wounded in a thwarted suicide attack at a city hospital in eastern Afghanistan. The suicide bomber, wearing a doctor’s white coat, was wrestled to the ground by NATO troops just after a crowd of 150 people were able to flee safely (USA Today 2007).

- On February 25, 2004, a Haitian hospital was visited by a group of 20 armed men who threatened the medical staff and patients and disarmed the security guard (MSF 2004).

- In August 2003, at least 27 people were killed in a suicide bombing in the Russian city of Mozdok. A suicide bomber drove a truck filled with explosives through the gates of a military hospital and detonated the explosives (CNN.com 2003).

- In August 2002, four nurses died and at least 20 were injured in a suicide grenade attack at a hospital in Pakistan (CNN.com 2002).

- Incidents of weapons brought into and used in hospitals are not uncommon. Accounts of various shootings are summarized at the Web sites listed below. These instances involved the shooting of a single victim in a hospital setting and were not terrorist or hostage-taking incidents (The Florida Times-Union 2006; 6abc.com 2005; TheBostonChannel.com 2003; Burchette 2000).

Consequences of an Event

The consequences of a successful attack on hospitals can be wide-ranging. Consequences include those that follow.

Public Health and Safety Consequences

A terrorist attack on a hospital could result in a large number of deaths and injuries. In a bombing attack, the number of casualties would greatly increase if the blast was strong enough to cause building collapse. If a biological agent was dispersed throughout a hospital, the casualties would occur more gradually, and impacts could be mitigated if prophylaxis for the agent were available. In the case of a communicable disease, impacts would also be mitigated if isolation facilities and procedures were adequate. In a biological attack on a hospital, the agent could be spread to the community through hospital staff or patient visitors.

A terrorist attack on a hospital, whether a bombing, chemical agent, or bioterrorism attack, would also impact local and regional emergency and public health services. Many fire-and-
rescue, HAZMAT, law enforcement, and medical personnel, facilities, and equipment might need to be activated. The impact would depend on the availability of other local health-care providers and on the services that had been damaged. For example, damage to a Level 1 trauma center could have particularly high negative impacts on regional trauma health services.

**Economic Consequences**

The costs of a terrorist attack on a hospital could be very high for victims and families, hospital owners, and insurance companies. Local governments could also incur high costs from emergency services rendered after an attack.

**Social and Institutional Consequences**

A large-scale attack on a hospital that caused many casualties could result in a fear of using hospital services among the general public. There could be widespread general anxiety stemming from the feeling that an institution generally thought of as a place of refuge and safety was no longer safe. Individuals might also attempt to treat injuries or conditions at home or at small clinics, resulting in adverse outcomes for some patients.
STANDARDS AND REGULATIONS

Hospitals of all sizes and layouts must follow local and/or state general building codes, except for federal facilities, which must follow federal regulations. Forty states have adopted the American Institute of Architect’s Guidelines for Design and Construction of Hospitals and Health Care Facilities (AIA 2001) as a standard. These guidelines specify that:

Owners of existing facilities should undertake an assessment of their facility with respect to its ability to withstand the effects of regional natural disasters. The assessment should consider the performance of structural and critical nonstructural building systems and the likelihood of loss of externally supplied power, gas, water, and communications under such conditions. Facility master planning should consider mitigation measures required to address conditions that may be hazardous to patients and conditions that may compromise the ability of the facility to fulfill its planned post-emergency medical response.

As components of this emergency planning, the guidelines give certain requirements. For example:

- Facilities should designate an outdoor location with plumbing and drainage adjacent to the ER as a decontamination area.

- If normal operations are interrupted, facilities should have supplies stored on hand to allow for at least four continuous days of operation (supplies include food, sterile supplies, pharmacy supplies, and water for sanitation).

- One or more airborne infection isolation rooms should be provided in emergency services, the critical care unit, the pediatric and newborn intensive care units, surgical care suites, and other hospital areas, as specified in hospital-specific, infection-control risk assessments.

Specifications for isolation rooms are given in the guidelines document (AIA 2001).

Hospitals with Medicare patients must also meet federal government standards, and accredited hospitals must meet the standards of the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) and pass the JCAHO inspections.

Because hospitals are considered to be “essential buildings” that must be able to maintain operations in the event of a disaster (natural or man-made), the structures are subject to higher structural and safety requirements than other buildings (Kliment et al. 2000). For example, most states have special requirements for provision of emergency power, such as adequate on-site fuel storage, uninterruptible power systems, separate smoke compartments on each floor, and adequate corridor widths to facilitate evacuations. In California, where seismic activity is of concern, new inpatient facilities must be built to remain operational after an 8.0 earthquake.
**PROTECTIVE MEASURES**

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures are designed to meet one or more of the following objectives:

- **Devalue**: Lower the value of a facility to terrorists; that is, make the facility less interesting as a target.
- **Detect**: Spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.
- **Deter**: Make the facility more difficult to attack successfully.
- **Defend**: Respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack.

Many different protective measures are available for deployment at a facility and in the areas surrounding a facility (buffer zones). Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or a specific threat stream. In addition, some may be tactical in nature, while others may address long-term strategic needs (e.g., redundancy).

Some protective measures are designed to be implemented on a permanent basis to serve as routine protection for a facility. Such measures are sometimes referred to as ‘baseline countermeasures.’ Others are either implemented or increased in their application only during times of heightened alert.

The implementation of a protective measure at any time involves the commitment of resources in the form of people, equipment, materials, time, and money. Facility owners, local law enforcement personnel, emergency responders, and state and local government agencies need to coordinate and cooperate in determining what measures should be implemented, how extensive they should be, and how long they should be kept in force in order to maximize security while staying within the bounds of available resources.

To assist in the decision process, the U.S. Department of Homeland Security (DHS) has developed the color-coded Homeland Security Advisory System (HSAS) to communicate with public safety officials and the public at large so that protective measures can be implemented or expanded to reduce the likelihood or impact of an attack. Table 1 shows the HSAS alert levels.

When the available intelligence allows, HSAS alerts are supplemented by information on the threat stream(s) most likely to be used by terrorists. This information may or may not be very specific, may or may not identify geographic areas of concern, and may or may not offer a time period when attacks might be expected. This level of uncertainty is inherent in dealing with
terrorist threats and must be factored into decisions on committing resources to implement protective measures.

Table 1 DHS Advisory System Alert Levels

<table>
<thead>
<tr>
<th>Alert Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>SEVERE</td>
</tr>
<tr>
<td>Orange</td>
<td>HIGH</td>
</tr>
<tr>
<td>Yellow</td>
<td>ELEVATED</td>
</tr>
<tr>
<td>Blue</td>
<td>GUARDED</td>
</tr>
<tr>
<td>Green</td>
<td>LOW</td>
</tr>
</tbody>
</table>

The measures shown on the following charts are designed to provide information and assistance to facility owners, site managers, local law enforcement personnel, and state and local homeland security agencies in making decisions on protective measures. These suggested measures are collated from infrastructure-specific guidance and from experience in a number of localities across the country. The following should be noted regarding the suggested protective measures:

- These measures are intended as a guide; they are not a requirement under any regulation or legislation. In addition, because of the wide variety in the types of facilities, not all suggested measures will be applicable.

- These suggestions are based on practices employed by facilities across the nation. The ability to implement them at any specific facility will vary.

- These suggestions should not be viewed as a complete source of information on protecting facilities. Facility managers and local security personnel should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

The protective measures are grouped into the following categories:

- Planning and Preparedness
- Personnel
- Access Control
- Barriers
- Communication and Notification
- Monitoring, Surveillance, Inspection
- Cyber Security
- Infrastructure Interdependencies
- Incident Response
PLANNING AND PREPAREDNESS

These measures relate to emergency plans and preparations.

- Designate an experienced employee as security director to lead all security-related activities.
- Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis. Include assessments of other activities and operations in the vicinity (e.g., airports, chemical plants, government buildings, pipelines, rail lines) to determine whether these facilities have any potential to increase security risks to the hospital. On the basis of these analyses, develop a comprehensive security plan and emergency response plan for the hospital. Include:
  - Standard operating procedures (SOPs) to cover all potential emergency situations, including the possibility of multiple events (e.g., explosives attack and loss of electric power).
  - An identification of security responsibilities and a chain-of-command for incident response.
  - Operations Security (OPSEC) procedures to cover routine security activities by all staff.
  - Procedures for dealing with people who have special needs (e.g., with physical disabilities, non-English-speaking).
- Coordinate plans with appropriate agencies and support them with mutual aid agreements.
- Involve employees at several levels in security planning. Consider a third-party evaluation of plans.
- Develop business recovery/continuity plans to be implemented in the aftermath of an incident.
- Test security, emergency, and continuity plans regularly with drills and tabletop exercises.
- Establish liaisons and regular communication with local law enforcement personnel and emergency responders, state and federal law enforcement and terrorism agencies, other public health organizations, and industry organizations to enhance information exchange, clarify emergency responses, track threat conditions, and support investigations.
- Consider establishing an emergency operations center to coordinate resources during an incident.
- Keep and protect copies of the security and emergency response plans in redundant locations.
- Restrict access to sensitive facility data and information (e.g., building plans, life safety systems).
- Develop policies and procedures for dealing with the media and the general public in the event of an incident to advise them of the situation and to defuse rumors and panic.
- Establish procedures for facility evacuation and for shelter-in-place situations. For shelter-in-place situations, ensure that there is a shelter that is adequately stocked to accommodate the number of people who might need to use it.
- Develop procedures for shutting down the facility if the threat is deemed too serious to continue operations.

**During Periods of High Alert (HSAS ORANGE):**
- Review and implement actions specified in the security and emergency response plans. Adjust them as necessary to deal with specific threat information.
- Activate the facility emergency operations center as appropriate.

**During Periods of Severe Alert (HSAS RED):**
- Review available threat information and determine if the facility should be closed or should operate with reduced hours, a reduced workforce, and/or reduced activities.
PERSONNEL
These measures relate to personnel.

Employees

- Conduct background checks on all employees. Conduct more detailed checks on those who will have access to critical assets. Develop a list of disqualifying factors.
- Incorporate security awareness and appropriate response procedures for security situations into employee training and refresher programs. Include SOPs in the security and emergency response plans; recognize and maintain alertness with regard to situations that may pose a security threat; develop contact and notification protocols for suspicious situations and emergencies; maintain caution about providing facility information to outsiders; and develop procedures to provide for the safety of employees during an incident.
- Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., irregular work hours, attempts to access restricted areas).
- Review the personnel files of recently terminated staff members to determine if they pose a security risk.

Security Force

- Maintain an adequately sized, equipped, and trained security force.
- Coordinate security force operations with local law enforcement and other agencies.
- Develop a security force patrol schedule that includes both regular and random patrols.

Contractors, Vendors, Temporary Employees

- Provide security information and training to all nonemployees visiting the facility. Advise them to be alert to suspicious activity or items and advise them on how to report suspicious incidents.
- Require contractors, vendors, and temporary employment agencies to vouch for the background and security of their personnel who will visit the facility.

During Periods of High Alert (HSAS ORANGE):

- Provide additional reminders to employees and visitors about the security situation.
- Increase the security force presence and extend patrols to a wider perimeter.
- Consider augmenting security with special units (e.g., armed guards, K-9 units).
- Activate the emergency operations center.
- When appropriate, have employees, especially those working in remote or isolated areas, work in pairs.

During Periods of Severe Alert (HSAS RED):

- Increase the security force presence to the maximum level sustainable.
- Request support from law enforcement personnel and, if appropriate, the National Guard.
**ACCESS CONTROL**

These measures relate to controlling critical facility access. (Consideration should be given before implementing access control measures. Typical security upgrades may impede the purpose of the facility, which is to provide 24/7 public access to those in need of care.)

### General Measures

- Define the facility perimeter and areas within the facility that require access control for pedestrians and vehicles. Identify especially critical areas (e.g., control rooms, fuel or chemical storage areas, shipping docks, utility rooms) that require special access controls (e.g., logging of entry/exit).
- Train security staff to identify prohibited items (e.g., firearms, explosives). Train mail room and receiving personnel to recognize suspicious mail, packages, or deliveries.
- Enforce access control measures (e.g., locking of buildings not in use). Implement rigorous key control procedures. Secure master keys. Secure all tools that could be used to force entry into a critical area (e.g., bolt cutters, cutting torches).

### Employees

- Issue photo ID badges to all employees. Require that badges be displayed at all times and verified to gain access to critical areas. Use an electronic access tracking system to log entry and exit from critical facilities. Collect employee badges and keys when employment is terminated.

### Contractors, Vendors, Temporary Employees

- Issue special ID badges to known and expected contractors, crews, vendors, and temporary employees. Require that badges be displayed at all times and verified to gain access to critical areas. Collect all badges when visits are complete.

### Vehicles

- Issue employee parking permits for designated areas. Lock facility vehicles when not in use.
- Approach illegally parked vehicles and require them to be moved or towed.

### During Periods of High Alert (HSAS ORANGE):

- Reduce the number of site access points and increase the security force presence.
- Delay nonessential contractor work.
- Restrict parking to areas away from critical assets.
- Accept deliveries only during daytime hours and away from critical facilities.

### During Periods of Severe Alert (HSAS RED):

- Consider closing the facility to new patients until the threat has been reduced.
- Halt contractor work, special tours, and nonessential mail, shipments, and deliveries.
- Freeze all movement of vehicles close to patient care facilities except for security and emergency response.
**BARRIERS**
These measures relate to physical barriers and barricades.

<table>
<thead>
<tr>
<th>Building Barriers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establish a clear zone adjacent to critical buildings. Keep the zone free of</td>
</tr>
<tr>
<td>vegetation and other obstructions to allow for continuous monitoring and to</td>
</tr>
<tr>
<td>inhibit concealment of people or packages.</td>
</tr>
<tr>
<td>• If appropriate, install building perimeter barriers (e.g., fences, bollards,</td>
</tr>
<tr>
<td>large flower pots) around critical buildings.</td>
</tr>
<tr>
<td>• If appropriate, install interior building barriers (e.g., internal locked doors)</td>
</tr>
<tr>
<td>to protect sensitive or critical areas or corridors within a building (e.g.,</td>
</tr>
<tr>
<td>blood bank).</td>
</tr>
<tr>
<td>• Ensure that exterior doors have hinge pins that cannot be removed from the</td>
</tr>
<tr>
<td>outside and that there are no gaps between the door and jamb that would allow</td>
</tr>
<tr>
<td>the door to be compromised.</td>
</tr>
<tr>
<td>• Install barriers at HVAC systems (e.g., screens on intakes, filters) to prevent</td>
</tr>
<tr>
<td>the introduction of CBR agents into the building. Train staff in emergency</td>
</tr>
<tr>
<td>shut-off procedures for HVAC systems.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vehicle Barriers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Install bollards on pedestrian walkways to keep vehicles off of them.</td>
</tr>
</tbody>
</table>

**During Periods of High Alert (HSAS ORANGE):**
- Where appropriate, deploy temporary barriers (e.g., Jersey barriers, heavy vehicles and equipment, empty containers) to increase the standoff distances from critical areas.

**During Periods of Severe Alert (HSAS RED):**
- Increase the number and security of barriers to the maximum extent possible consistent with the operating level of the facility.
### COMMUNICATION AND NOTIFICATION

These measures relate to communications.

#### Communications Equipment
- Install systems that provide communication with all people at the facility, including employees, the security force, emergency response teams, and visitors. Provide redundant communication channels and backup sources of power for these systems. Test systems regularly.
- Install systems that provide communication channels with local law enforcement personnel and emergency responders. Test the systems regularly.
- Provide communication capability for employees who are at adjacent hospital buildings.
- Provide communication security (e.g., encryption, multiple frequencies) that will prevent unauthorized interception of information. Train employees not to discuss sensitive information over communication channels that are not secure (e.g., cell phones).
- Provide the ability to record incoming telephone calls to identify potential threats.

#### Communication Protocols
- Develop a notification protocol that outlines who should be contacted in emergencies. Regularly test the notification protocol through drills and exercises.
- Provide a simple and straightforward means for people to communicate the presence of a potential threat or an emergency (e.g., hotline number, internal 9-1-1 capability).
- Develop a process to update on- and off-duty employees about the current security situation.
- Establish call-in procedures for employees who work in remote or isolated locations.
- Develop a process for communicating with the public and the media regarding security issues. Provide adequate information to quell rumors and dispel unnecessary alarm. Take steps to restrict the release of information that might compromise the security posture of the facility.

#### Information Sharing
- Monitor industry and government information on threats, incidents, and response procedures. As appropriate, share information on the facility’s experiences.

**During Periods of High Alert (HSAS ORANGE):**
- Increase the frequency of communications with local law enforcement personnel.
- Increase communications about the security situation with employees and visitors.
- Increase the frequency at which employees working in remote areas report.

**During Periods of Severe Alert (HSAS RED):**
- Maintain communication with local law enforcement personnel as continuously as is sustainable.
- Provide employees and visitors with as much information as possible as often as possible to keep them apprised of the security situation.
- Activate backup equipment so it is ready to use in the event of an incident.
### MONITORING, SURVEILLANCE, INSPECTION

These measures relate to procedures and equipment used to monitor the movements of people, vehicles, and materials.

#### Equipment
- Provide visual surveillance capability for critical areas. Train staff to watch for unusual activities.
- Install video surveillance equipment (e.g., closed-circuit television [CCTV]). Provide coverage for critical areas, roadways, parking lots, and entrances. Install intrusion, motion, and other detectors (e.g., fire, smoke) as appropriate. Maximize the recording time. Establish procedures to secure video and other incident data for forensic purposes. Test regularly.

#### Buildings and Facility Assets
- Regularly inspect the site perimeter, buildings, equipment, and critical areas for signs of security issues. Implement random and scheduled inspections. Include assets not used frequently.

#### People
- Monitor people entering and leaving the facility. Train monitors to detect suspicious behavior.
- Monitor the activities of contractors, delivery personnel, and vendors for unusual behavior.
- Where practical, provide inspections of people entering and leaving critical areas.

#### Vehicles
- Monitor vehicles approaching the facility for signs of threatening behavior.

#### Deliveries and Mail
- Supervise the unloading of materials and equipment. Verify the shipper and delivery details.
- Conduct more thorough inspections of deliveries involving HAZMAT or sensitive materials.
- Inspect mail for unusual signs. Provide PPE to mail-handling staff.
- Advise key employees to check deliveries and mail at home for suspicious material.

#### Materials
- Maintain a thorough inventory and accounting of all sensitive items and their storage and use.

**During Periods of High Alert (HSAS ORANGE):**
- Increase monitoring, surveillance, inspections, and lighting. Reassign staff to assist.
- Isolate or remove any HAZMAT that might increase the impacts of an attack.

**During Periods of Severe Alert (HSAS RED):**
- Increase the frequency and thoroughness of surveillance, monitoring, and inspection activities to the maximum level. Request additional support from local law enforcement agencies.
- Inspect mail/deliveries. Postpone nonessential deliveries.
**CYBER SECURITY**

These general measures relate to protecting data, process controllers, computers, and networks.

- Implement adequate policies, procedures, and culture regarding cyber security.
- Maintain a well-trained computer security staff with the appropriate knowledge and experience to deal with cyber security issues. To secure specific devices and systems, regularly consult with trade organizations, vendors, or specialists about cyber security practices, standards, and strategies. Conduct thorough background checks on employees serving as system administrators.
- Validate the credentials and work of contractors and vendors given access to technology systems.
- Install and maintain up-to-date cyber security techniques, software patches, and strategies:
  - Ensure that systems and networks have sufficient defense-in-depth mechanisms.
  - Provide audit and forensic capability, with easy tools for detecting inappropriate activity.
  - Ensure that critical host computers do not have inappropriate applications (e.g., games) installed.
  - Enforce password procedures (e.g., frequency of change, strength, and password reuse).
  - Provide adequate control over remote access and modems (e.g., land-line and wireless).
  - Back up data and configuration files regularly. Maintain backups in a separate/secure location.
  - Develop redundancy in technology hardware and software to keep critical systems operating.
  - Develop a recovery plan to return systems to full functionality after an incident.
  - Regularly review the facility Web site to ensure that no sensitive information is provided.
- Provide training to all employees who use computer systems on cyber security policy, procedures, responsibilities, threats, and incident reporting. Immediately cancel access for terminated staff.
- Control physical access to critical technology facilities and devices (e.g., computer rooms).
- Regularly test cyber security measures (e.g., audits, penetration testing, war-dialing, tabletop exercises).

**During Periods of High Alert (HSAS ORANGE):**
- Delay scheduled maintenance and upgrades; increase frequency of system backups.
- Increase system monitoring; ask employees to increase vigilance with regard to unusual activities.
- Reduce access to the Internet; restrict instant messaging and peer-to-peer applications.
- Commit the time of technical support personnel to deal with any problems.

**During Periods of Severe Alert (HSAS RED):**
- Increase computer security to maximum levels.
- Reduce access to the Internet and other portals to the absolute minimum.
- Have technical support available on call 24/7.
- Consider disabling the facility’s Web site.
**INFRASTRUCTURE INTERDEPENDENCIES**
These measures relate to the protection of vital utilities that support operations at the facility.

- Ensure that the facility has adequate utility service capacity to meet normal and emergency needs. Identify all utility service points that support the facility. Establish regular communication channels with utility service providers (e.g., electric, gas, water, telecommunications, trash collection companies) to review existing systems, capacity expansion needs, and actions to be taken in response to loss of service from primary supply sources and during other emergencies.
- Provide for redundancy and emergency backup capability for critical utility services (e.g., backup electric power generators, multiple utility feeder lines). Where possible, locate the redundant and backup equipment in a different part of the facility from the one that houses the primary supply equipment. Inspect, maintain, and test redundant and backup equipment regularly.
- Ensure that employees are familiar with how to shut off utility services (e.g., electricity, natural gas) in emergency situations.
- Provide adequate physical security (e.g., fencing, locks, protective enclosures, access restrictions) for utility services, fuel storage containers, trash dumpsters, and HVAC systems. Include installation of special locking devices on utility access points (e.g., manhole covers, HVAC vents).
- As much as practical, put utility supply facilities that are potentially hazardous (e.g., liquid fuel tanks) a safe distance from buildings and areas where large numbers of people congregate.
- Provide for regular monitoring and inspection of utility service areas (e.g., security patrols, CCTV).
- Secure dumpsters and other trash containers to prevent the hiding of explosives or other HAZMAT and to prevent unauthorized access to discarded papers and records.

**During Periods of High Alert (HSAS ORANGE):**
- Increase monitoring, inspection, testing, and patrols of all utility services. Request assistance from local law enforcement personnel.
- Establish communication with utility service providers to review plans for responding to any disruptions.

**During Periods of Severe Alert (HSAS RED):**
- Provide continuous monitoring of all utility services. Consider providing a continuous security guard presence at critical utility points.
**INCIDENT RESPONSE**
These measures relate to preparations for responding to an actual incident.

- Develop and maintain an up-to-date emergency response plan (see Planning and Preparedness), incident notification process, and emergency ‘calling trees’ that cover all staff.
- Ensure that there are backup personnel who can execute emergency response functions if primary personnel are unavailable. Ensure that equipment and supplies are adequate to support emergency response requirements; keep them secure and check their status periodically.
- Prepare an emergency operations center to coordinate resources during an incident.
- Conduct regular training, drills, and tabletop exercises with emergency response teams. Involve local emergency responders in drills and exercises.
- Encourage employees to participate in community and other outside organization emergency preparedness and response training.
- Identify entry and exit points to be used in emergencies. Ensure that they are free of obstructions and can be fully utilized. Train all employees on the location of these points.
- Establish procedures for facility evacuation and for shelter-in-place situations. Identify rendezvous points for employees and patients to gather for ‘head counts’ after an evacuation.
- Ensure that local law enforcement personnel and emergency responders know the names of and contact information for security and crisis management leaders at the facility.
- Develop policies and procedures for dealing with the media and the general public in the event of an incident to advise them of the situation and to defuse rumors and panic.
- Develop plans to assist the families of facility response teams in the event the teams must be away from home for extended periods.
- Develop plans to provide counseling to employees in the aftermath of an incident.
- Implement procedure for capturing lessons learned and revising response plans after an incident.

**During Periods of High Alert (HSAS ORANGE):**
- Review and implement emergency response plans. Adjust as necessary for conditions.
- Activate the facility emergency operations center as appropriate; notify law enforcement personnel.
- Delay leaves or travel for critical facility personnel.
- Pre-position emergency response personnel and equipment to enable rapid response.
- Review and prepare contingency plans that may be needed (e.g., review procedures with employees assigned to direct facility traffic, direct crowd control, guide first responders [if they are needed], or shut off utilities during an incident).

**During Periods of Severe Alert (HSAS RED):**
- Review available threat information; determine if the facility should be closed/restricted.
- Bring the emergency operations center up to full capability on a 24/7 basis.
- Cancel all leaves and travel for facility personnel.
Reference Material


OTHER USEFUL INFORMATION


U.S. Department of Homeland Security


Other U.S. Government Agencies

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

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

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

Other Organizations

American Red Cross, 2006, Terrorism: Preparing for the Unexpected [http://www.redcross.org/services/disaster/0,1082,0_589_,00.html].


Note: Information presented here is subject to copyright laws and other terms of use as set forth in the respective references.
Dear Reader,

Please take a few minutes to complete this survey. Your input will be used to evaluate the quality and value of DHS products. It is important that this report series on Common Vulnerabilities (CV), Protective Measures (PM), and Potential Indicators of Terrorist Activity (PI) remain responsive to your needs.

Thank you.

<table>
<thead>
<tr>
<th>Circle your response accordingly:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Strongly Disagree</td>
</tr>
<tr>
<td>2 Disagree</td>
</tr>
<tr>
<td>3 Neither Agree or Disagree</td>
</tr>
<tr>
<td>4 Agree</td>
</tr>
<tr>
<td>5 Strongly Agree</td>
</tr>
<tr>
<td>NA Not Applicable</td>
</tr>
</tbody>
</table>

## Quality

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Information in this report is presented clearly and logically.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The content and documented sources make this report reputable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The LENS web site is easy to access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Information on the LENS web site is easy to navigate and find.</td>
</tr>
</tbody>
</table>

## Value

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>NA</th>
<th>This report is relevant to your mission, programs, priorities, or initiatives.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
<td>This report enhanced your knowledge of infrastructure protection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
<td>This report will likely result in changes to your existing protection practices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
<td>This report will likely result in more informed protection decisions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

## Comments

Title or type of report: ___________________________ Organization or reader name: _______________________

Mail or Fax to: Argonne National Laboratory
Infrastructure Assurance Center
9700 South Cass Avenue, Building 900
Argonne, IL 60439
Fax: 1-630-252-9559