RELIGIOUS FACILITIES:

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: May 2006

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

Infrastructure Protection Report Series
Religious Facilities

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

There are approximately 250,400 religious congregations in the United States, consisting of about 138 million members. These members comprise approximately 200 different religions or divisions of religions and meet weekly in more than 240,000 facilities across the country.

This report presents the following information related to religious facilities:

- Potential Indicators of Terrorist Activity
- Common Vulnerabilities
- Protective Measures
- Useful References

This report is one of a series of documents that address how our nation can better protect its critical infrastructures and key resources. In addition to this report, a companion document, *Overview of Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures for Critical Infrastructures and Key Resources* (DHS 2006), presents information gathered across a wide range of critical infrastructures. See contacts listed on cover page for additional information.

RELIGIOUS FACILITY CHARACTERISTICS

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

Characterization of the Segment

A study published by the Association of Statisticians of American Religious Bodies and entitled *Religious Congregations and Membership in the United States 2000* reports that the United States has approximately 250,400 religious congregations consisting of about 138 million members. These members comprise approximately 200 different religions or divisions of religions and meet weekly in more than 240,000 facilities across the country. The number of people coming and going during the week varies with the size of the congregation living nearby. In rural areas, congregations are generally small (100 members or less). In large metropolitan areas and suburbs, congregations can exceed 10,000 members. Some religious facilities also provide educational resources for students in prekindergarten and kindergarten through 12th grade. Some religious facilities, like the Washington National Cathedral, are national icons.

In Texas, a multimillion dollar expansion of an existing facility included a 6,400-seat worship center (Figure 1), a music suite with two choir and one orchestra rehearsal rooms, administrative offices, educational classrooms shared by Sunday Bible study and weekday private school (K–12), a bookstore and two libraries, and a large family recreation facility. Multiple services are held to provide seating for all of the members who want to attend.

Figure 1 Large Church Worship Center

Another large U.S. church has 22,000 members and an annual budget of $10 million. Its sanctuary seats 4,000. The large membership is attributable in part to its television ministry. One rapidly growing church has leased a sports arena (Figure 2) that it is transforming into a facility that will seat 16,000 for services; provide ice rink and basketball facilities for families and city leagues; and be used for concerts, sporting events, and conferences.

Larger facilities are often located in cities where the lead church of a denomination resides. The Mormon Conference Center in Salt Lake City seats 21,000 persons in its main sanctuary (Figure 3). These types of facilities accommodate large numbers of visiting members and host

Figure 2 Artist's Concept of Sports Arena Converted to a Religious Facility

Figure 3 Mormon Conference Center, Salt Lake City, Utah

congregational meetings and religious conventions, providing support and direction for their member congregations around the country.

Very large congregations are the exception rather than the rule. Most religious facilities are smaller buildings in which small and medium-sized congregations meet.

As reported on Adherents.com, a Web site that provides national and world religion statistics:

> Unlike some countries, the United States does not include a question about religion in its census, and has not done so for over fifty years. Religious adherent statistics in the United States are obtained from surveys and organizational reporting… The largest, most comprehensive surveys on religious identification were done [by] sociologists Barry A. Kosmin, Seymour P. Lachman, and associates at the Graduate School of the City University of New York. Their first major study was done in 1990: the National Survey of Religious Identification (NSRI). This scientific nationwide survey of 113,000 Americans asked about religious preference, along with other questions. They followed this up, with even more sophisticated methodology and more questions, with the American Religious Identity Survey (ARIS) conducted in 2001, with a sample size of 50,000 Americans.

Table 1 shows the distribution of religious affiliations in the United States based on the ARIS data. Religious facilities are located in every city and county throughout the United States.

Table 1 Distribution of Religious Affiliation in the United States

Religion	Estimated Adult Membership in 2001	Portion of U.S. Population (%)
Christianity	159,030,000	76.5
Nonreligious/Secular	27,539,000	13.2
Judaism	2,831,000	1.3
Islam	1,104,000	0.5
Buddhism	1,082,000	0.5
Agnostic	991,000	0.5
Atheist	902,000	0.4
Hinduism	766,000	0.4
Unitarian Universalist	629,000	0.3
Wiccan/Pagan/Druid	307,000	0.1
Spiritualist	116,000	
Native American Religion	103,000	
Baha'i	84,000	
New Age	68,000	
Sikhism	57,000	
Scientology	55,000	
Humanist	49,000	
Deity (Deist)	49,000	
Taoist	40,000	
Eckankar	26,000	

Source: http://www.adherents.com/.

Common Facility Characteristics

Religious facilities vary from small, single-story buildings or converted storefronts (see Figure 4), to medium-size facilities (Figure 5), to very large buildings (Figure 6). Most religious facilities have one or more meeting/worship areas for the congregation that can seat from 10 to tens of thousands of people.

In addition to the meeting areas, some religious facilities have classrooms and fellowship halls where food is served. Larger facilities may also have chapels, gymnasiums, craft areas, book stores, museum areas, religious libraries, and gardens. Most have heating, ventilating, and air-conditioning (HVAC) systems; electrical and telecommunication systems; and water, plumbing, and sewage systems.

Religious facilities in metropolitan areas and suburbs frequently provide parking areas. Most have only outdoor parking surrounding the facility. Some of the larger churches in metropolitan areas have attached or semi-attached parking garages or underground parking. Some use adjacent business garages during nonbusiness hours under special arrangement with the business owner.

Vehicles routinely stop in front of the entrances and exits of religious facilities to discharge or pick up passengers. Likewise, vehicles stop for deliveries and parcel pickup. In most cases, no physical barriers exist between roadways and the entrances. Larger religious facilities may even have a separate delivery area and loading dock. At most religious facilities, deliveries are made to a designated person in the church office.

Large religious facilities often have auxiliary buildings and/or facilities integrated into their main structure, including wellness centers, school/classroom buildings, office space, chapels, and kitchen/dining areas. These facilities add to the number of entrances and exits of the facility.

Figure 4 Typical Small Religious Facilities

Figure 5 Typical Medium-size Religious Facilities

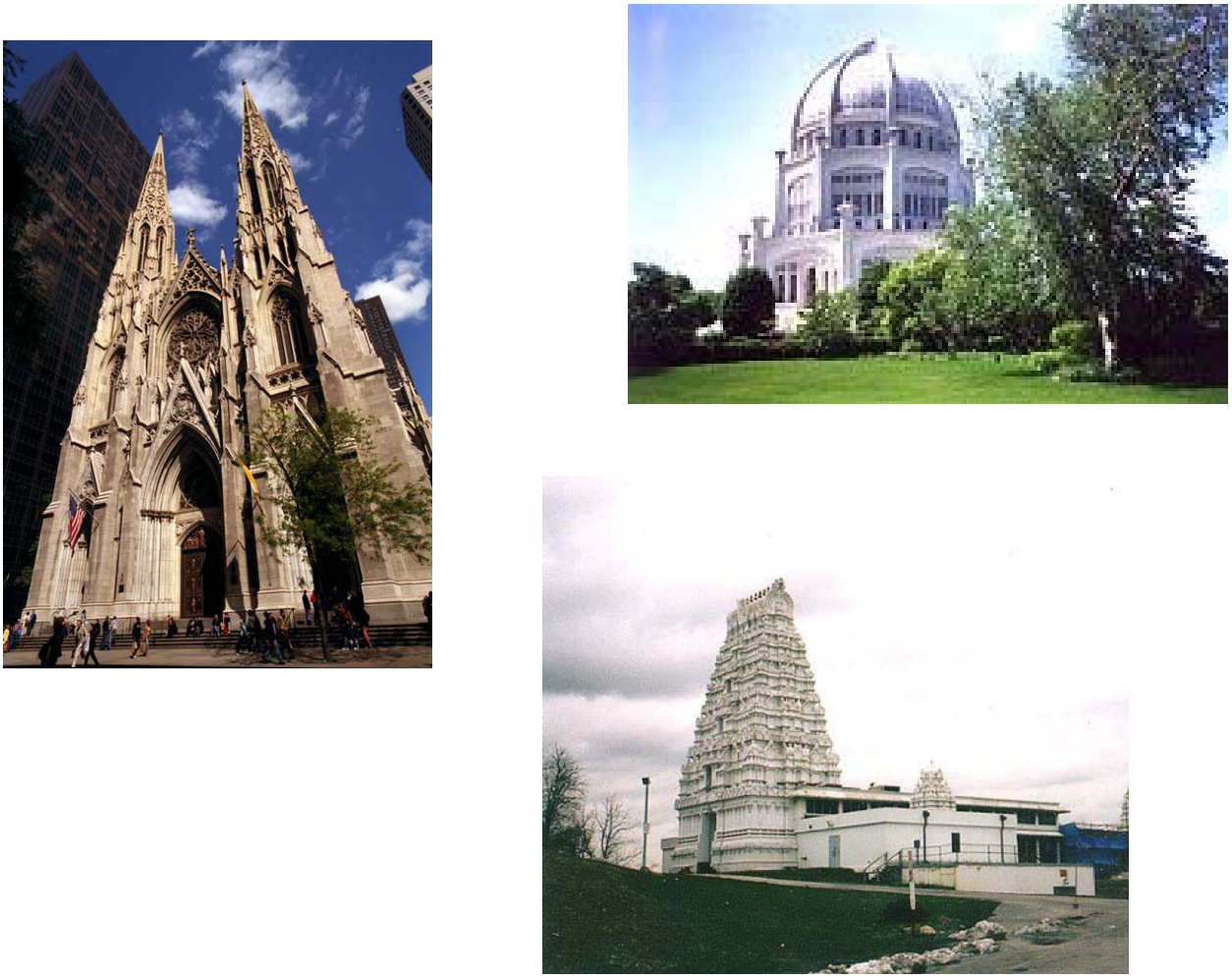

Figure 6 Typical Large Religious Facilities

To deter crime, some religious facilities have implemented tighter controls during office or school hours to limit access to small areas of the facility where a receptionist can greet all visitors. Some small religious facilities are completely locked down, and entrance can be gained only after a visitor is viewed through a closed-circuit television (CCTV) camera. However, during religious services, facilities are wide open with little or no access control, which could allow easy access for an adversary.

Most of the labor force at religious facilities consists of volunteers (e.g., greeters, teachers, choir and orchestra members, nursery workers, sound and television crews). Congregation religious leaders, office workers, and maintenance and cleaning crews may be employees, contractors, or a mixture, with some volunteers assisting as needed. Contractor firms are generally used to maintain the HVAC and other systems within the facility. Volunteer staff may not undergo background checks, except for nursery or school workers.

TERRORIST TARGETING OBJECTIVES, WEAPONS, AND TACTICS

Terrorists have a range of objectives in their attacks, as shown in Figure 7. Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many terrorist acts. Casualties can occur both at the facility that is attacked and in the surrounding area. Damage or destruction of the facility can be intended to (1) shut down or degrade the operation of the facility or (2) cause the release of hazardous materials to the surrounding area. Disruption of the facility without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. Theft of equipment, materials, or products can be intended to divert these items to other uses or to reap financial gain from their resale. Theft of information can be intended to acquire insight that is not made public or to gain data that can be used in carrying out attacks.

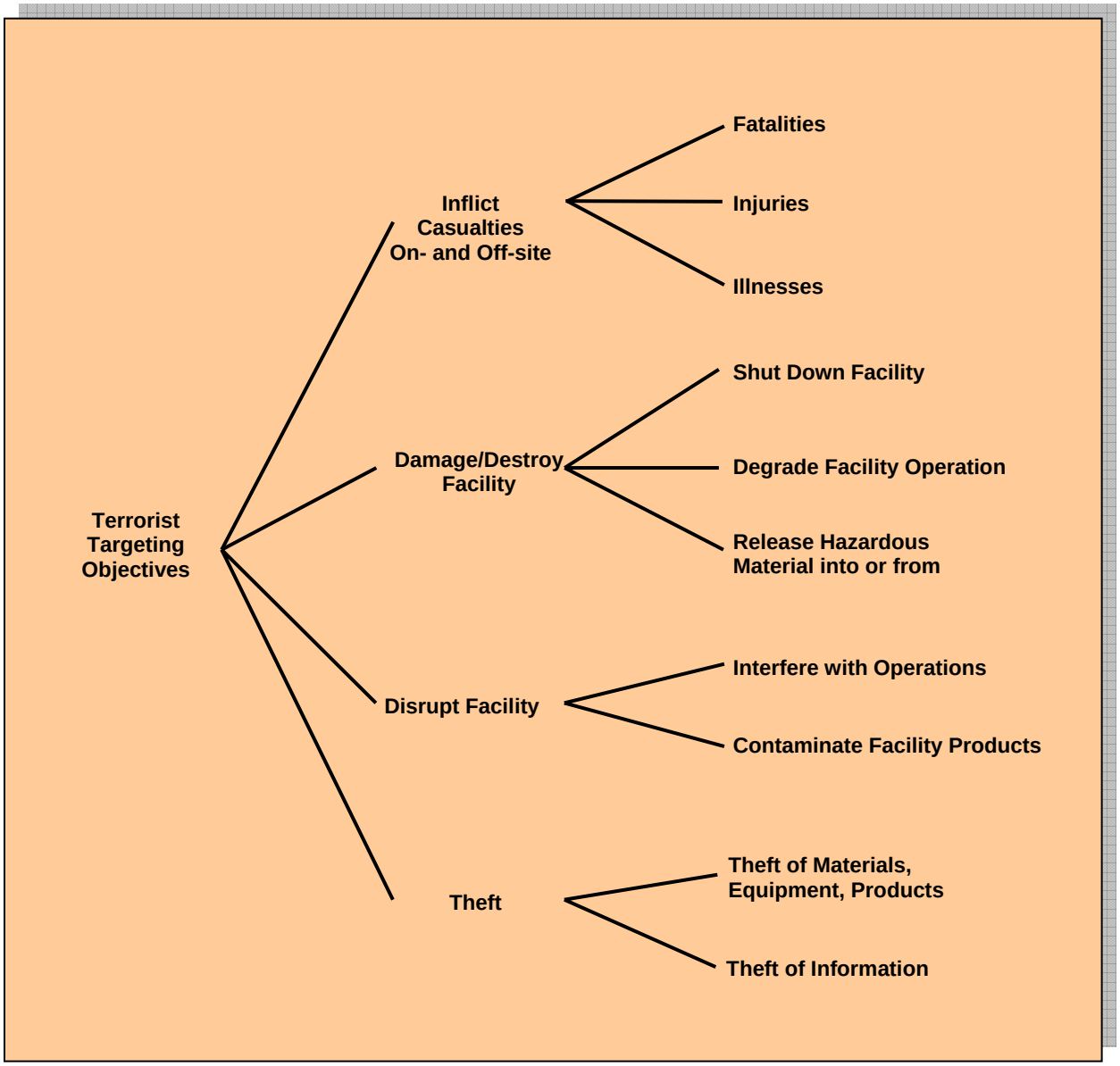

Figure 7 Terrorist Targeting Objectives

Terrorists have a wide variety of weapons and tactics available to achieve their objectives and have demonstrated the ability to plan and conduct complex attacks, simultaneously, against multiple targets. Attacks can be carried out by individuals, small teams of a few perpetrators, or larger groups acting in a coordinated fashion. The weapons and tactics include the following.

- ***Improvised Explosive Devices***

  An improvised explosive device (IED) (Figure 8), 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 can be deposited in an unnoticed location for detonation by a timer or by remote control. Vehicle-borne IEDs (VBIEDs) are loaded into a car or truck or on a motorcycle. The 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.

Array of Improvised Explosive Devices

Suicide Bomber

VBIED Car Bomb

Damage to the Federal Office Building, Oklahoma City, from a Truck Bomb

Figure 8 Examples of Improvised Explosive Devices

- ***Arson***

  Intentional fires can be set by using highly flammable materials (e.g., gasoline) tossed into a facility (see Figure 9). Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson is a threat both during and after normal business hours.

Figure 9 Arsonist Throwing a Fire Bomb

- ***Small Arms Attack***

  Attacks using conventional firearms, automatic weapons, shoulder-carried rocket-propelled grenades, or similar weapons can be aimed at indiscriminate shooting of people or at hostage taking (see Figures 10 and 11).

Figure 10 Conventional Small Arms

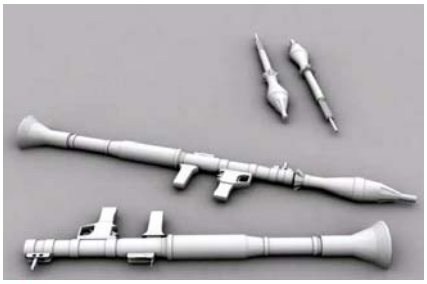

Figure 11 Rocket-Propelled Grenades and Launchers

- ***Assassination/Kidnapping***

  Many terrorist acts have involved the assassination of key personnel or the kidnapping of individuals and hostage-taking (see Figure 12).

Figure 12 Kidnapped Hostage

- ***Chemical Attack***

  Chemicals can be exploited or used by terrorists as a weapon. Such chemicals include toxic industrial chemicals that can be transported by truck or railroad to an area near a religious facility or near a large gathering of people then dispersed by explosives (Figure 13). 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 sarin gas attack in the Tokyo subway is an example (Figure 14).

Figure 13 Rail Tank Car Carrying Sulfuric Acid

Figure 14 Victims of Tokyo Subway Sarin Gas Attack, 1995

- ***Biological Attack***

  Biological pathogens (e.g., anthrax, botulin, plague) can cause disease and are attractive to terrorists because of the potential to cause mass casualties and exhaust response resources (Figure 15). Biological agents can be dispersed in the atmosphere (e.g., via crop dusting aircraft); can be introduced through a facility's HVAC system; or can be spread by contact (e.g., through contaminated letters delivered by mail) (Figure 16).

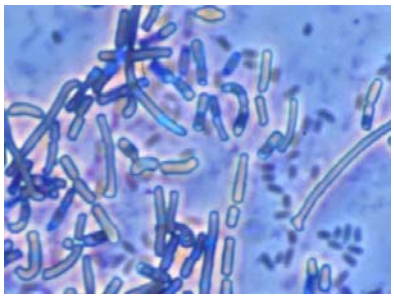

Figure 15 Anthrax Bacteria

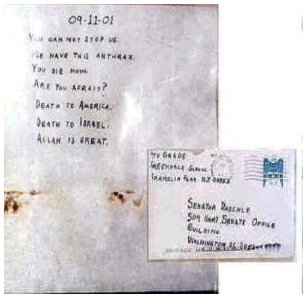

Figure 16 Anthrax-Laced Letter Sent to Senator Tom Daschle

- ***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 a variety of sources, such as medical or industrial equipment. All these agents can be introduced into a religious facility either directly (e.g., by spreading them on surfaces where people will have direct contact) or through the HVAC system. In radiological dispersion devices (RDDs), often called "dirty bombs," these materials are attached to an explosive to create a wide area of contamination (Figure 17).

Figure 17 Old Radioactive Material Container that Can Be Used as Part of an RDD

- ***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) (Figure 18). Some information systems can be used to mount attacks on other systems. Supervisory control and data acquisition (SCADA) systems that are used to control mechanical equipment can be infiltrated to operate the equipment in such a way as to cause damage and inflict on-site and off-site casualties (Figure 19).

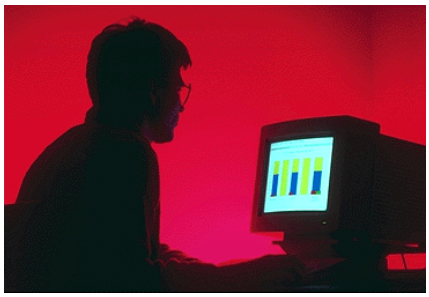

Figure 18 Hacker

Figure 19 SCADA System Control Room

Other threats, in addition to those listed above, may be of concern. A more comprehensive list of threat and weapon categories from many different critical infrastructures and key resources is provided in the Other Useful Information section at the end of this report.

POTENTIAL INDICATORS OF TERRORIST ACTIVITY

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack or that may be associated with terrorist surveillance, training, planning, preparation, or mobilization activities. The observation of any one indicator may not, by itself, suggest terrorist activity. Each observed anomaly or incident, however, should be carefully considered, along with all other relevant observations, to determine whether further investigation is warranted. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the facility of interest and what it might look like. The key factor in early recognition of terrorist activity is the ability to recognize anomalies in location, timing and character of vehicles, equipment, people, and packages.

The potential indicators can be grouped into the following categories:

- *Imminent Attack Indicators.* These indicators may show that an attack is imminent and that immediate action needs to be taken.

- *Surveillance Indicators.* These indicators may provide evidence that a facility is under surveillance by terrorists planning an attack.

- *Surrounding Area Indicators.* These indicators relate to activities in the area or region surrounding a facility and may demonstrate that an attack is being prepared.

The following sections describe these indicators. Every attempt has been made to be as comprehensive as possible in listing the indicators. Some of the indicators listed may not be applicable to every critical infrastructure or key resource. 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.

Imminent Attack Indicators

Indicators of an imminent attack include people, vehicles, and/or packages that demonstrate unusual and suspicious behavior that requires an immediate response. Some of the indicators of an imminent attack include the following:

- Persons in crowded areas (e.g., facility meeting areas) wearing unusually bulky clothing that might conceal suicide explosives. Such individuals might be patting down or feeling under their clothing, displaying electrical wires from under their clothing, tightly clutching an object that could be a trigger device, displaying excessive nervousness or anxiety, wearing an excessive amount of cologne or perfume to mask the scent of explosives, or concealing weapons (e.g., automatic rifle) under their clothing.

- Persons or teams of people spotted in or around the religious facility attempting to gain illegal entry (e.g., scaling fences, breaking into doors) or appearing to prepare to launch stand-off weapons (e.g., rocket propelled grenades) at the facility.

- Vehicles (e.g., cars, motorcycles, or trucks) illegally parked near religious facility buildings or near places where large numbers of people gather. The larger the vehicle, the larger the quantity of explosives that might be loaded into it. The vehicle may be unattended or may have a driver who will detonate it. The driver may demonstrate nervousness and anxiety and may be constantly scanning the area for law enforcement and/or to identify a location where a detonation will cause the largest number of victims.

- Unexpected or unfamiliar delivery trucks arriving at the religious facility.

- Vehicles approaching the facility at unusually high speed and/or steering around barriers and traffic controls.

- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives. Packages may be left in open areas or may be hidden in trash receptacles, lockers, or similar containers.

- Suspicious packages and/or letters received by mail that might contain explosives or chemical/biological/radiological agents. The packages or mail may have no return address, may have excessive postage, may have been sent from outside the United States, may have indications of liquids leaking from the package, or may have unusual odors.

- Evidence of unauthorized access to HVAC areas of a religious facility building. There may be indications of unusual substances (e.g., unknown powders, droplets, mists) near air intakes.

- 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.

Surveillance Indicators

Indicators of potential surveillance by terrorists include persons or unusual activities in the vicinity of a religious facility intending to gather information about the facility or its operations and protective measures. Terrorist surveillance may be fixed or mobile. Fixed surveillance is conducted from a static and 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 or choose disguises or occupations, such as street vendors, tourists, repair- or deliverymen, photographers, or even demonstrators, to provide a plausible reason for being in the area.

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

Progressive surveillance is a technique whereby the terrorist observes a target for a short time from one position, withdraws for a time (possibly days or even weeks), and then resumes surveillance from another position. This activity continues until the terrorist determines 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. 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 parks and other public gathering areas provide convenient venues for surveillance because it is not unusual for individuals or small groups in these areas to loiter or engage in leisure activities that could serve to cover surveillance activities.

Terrorists are also known to use advanced technology, such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices and global positioning systems. It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance refers to information gathering, legal and illegal, by terrorists using off-site computers. Types of data gathered might include site maps, key facility locations, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect data (e.g., damage or modify), software (e.g., damage or modify), or equipment/process controls (e.g., damage a piece of equipment). An electronic attack could be an end in itself or could be launched simultaneously with a physical attack.

Another surveillance tactic used by terrorists is the interception of radio or telephone (including cell phone) traffic. Equipment to conduct this type of surveillance is readily available.

Some of the indicators that a facility may be under surveillance by terrorists include the following:

Suspicious Person Behavior

- Persons using or carrying video/camera/observation equipment in or near the religious facility over an extended period.
- Persons discovered with religious facility maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel.
- Persons possessing or observed using night-vision devices near the facility perimeter or in the local area.
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
- Persons questioning religious facility employees off-site about practices pertaining to the facility and its operations, or an increase in personal e-mail, telephone calls, faxes, or postal mail requesting information about the facility or one of its key assets.
- Persons questioning religious facility employees or electric, natural gas, water or telecommunication employees about the facility's supporting infrastructure (e.g., electricity supply lines, natural gas lines, water supply).
- Observations of unauthorized personnel collecting or searching through the facility's trash.

Suspicious Employee Behavior

- Religious facility employees inquiring about facility operations, equipment, assets, or security measures about which they should have no job-related interest.
- Facility employees using video/camera/observation equipment that is not job-related.
- Facility employees found in possession of facility maps, photos, or diagrams that are not job-related.
- Facility employees associating with suspicious individuals.
- Employees changing working behavior or working more irregular hours.

- Increase in violations of security guard standard operating procedures for staffing key posts.

Suspicious Activities Observed or Reported

- An increase in threats from unidentified sources by telephone, postal mail, or the e-mail system and/or an increase in reports of threats from outside known, reliable sources.

- An increase in religious facility buildings left unsecured or doors left unlocked, when they are normally secured and locked at all times.

- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services and designed to determine the emergency responders' procedures.

- A noted pattern of equipment failures with indications of potential sabotage. These may be designed to test the religious facility's operations under such failure conditions or may be part of an actual attempt to disrupt the facility.

- Unfamiliar cleaning crews or other contract workers with passable credentials, or crews or contract workers attempting to access unauthorized areas.

- Unusual and unexpected maintenance activities (e.g., road repairs) near the religious facility or asset.

- Sudden increases in power outages designed to test the backup systems or recovery times of primary systems.

- Displaced or misaligned manhole covers or other service access doors on or surrounding the religious facility or asset site.

- Increased volume of downloading of materials (e.g., maps, photographs, schematics, or similar materials) from public computer sites that could be used in conjunction with surveillance or attack planning activities.

- Evidence of computer hackers attempting to access protected computer sites to look for personal information, maps, or other targeting examples. Repeated attempts from the same location or country to access protected computer information systems.

Surrounding Area Indicators

In addition to indicators that might appear at a facility itself, there are indicators that may appear in the communities surrounding a religious facility that should be considered and factored into decisions regarding security. The area of interest may be relatively large (e.g., 100 to 200 miles

around the facility). These indicators are generally identified by local law enforcement. Religious facility operators can establish communication channels with these organizations in order to maintain awareness of potentially threatening situations in the area and to piece together information from their facility with information from the surrounding area. Indicators that can be monitored include the following.

Weapons Indicators

Weapons indicators include the purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out an attack. Items of interest include not only guns, automatic weapons, rifles, etc., but also ammunition and equipment, such as night-vision goggles and body armor and relevant training exercises and classes. Indicators include the following:

- Thefts, losses, or sales of large numbers of automatic, semi-automatic, or large caliber (.50 caliber or greater) weapons in the surrounding area.
- Thefts or sales of ammunition capable of being used in military weapons in the surrounding area.
- Reports of automatic weapons firing or unusual weapons firing in the surrounding area.
- Law enforcement seizures of modified weapons or equipment used to modify weapons (silencers, etc.).
- Thefts, sales, or reported seizures of night-vision equipment in combination with other indicators.
- Thefts, sales, or reported seizures of body armor in combination with other indicators.
- Paramilitary groups carrying out training scenarios and groups advocating violence.
- People wearing clothing that is not consistent with the local weather (also applicable under all other indicator categories).

Explosives and Incendiary Indicators

Explosives and incendiary indicators include the production, purchase, theft, testing, or storage of explosive or incendiary materials and devices that terrorists could use to help to carry out the intended action. Also of interest are containers and locations where production could occur. Indicators include the following:

- Persons stopped or arrested in the surrounding area with unexplained large amounts of explosives.

- Inappropriate inquiries regarding explosives, including construction explosives, by unidentified persons.

- Thefts or sales of unusually large amounts of smokeless powder, blasting caps, or high-velocity explosives to unidentified persons.

- Sales of large amounts of high-nitrate fertilizer to nonagricultural purchasers or abnormally large amounts to agricultural purchasers.

- Thefts or sales of large amounts of combinations of ingredients that can be used for explosives (e.g., fuel oil, nitrate fertilizers) to unidentified persons and in quantities beyond normal.

- Thefts or sales of containers (e.g., propane bottles) or vehicles (e.g., large trucks, cargo vans — in particular, 1-ton capacity or greater) in combination with other indicators.

- Reports of explosions, particularly in rural or wooded areas.

- Seizures by local law enforcement of IEDs or materials.

Chemical, Biological, and Radiological Indicators

Chemical, biological, and radiological indicators include activities related to production, purchase, theft, testing, or storage of dangerous chemicals and chemical agents, biological species, and hazardous radioactive materials. Indicators include the following:

Chemical Agent Indicators

- Inappropriate inquiries regarding chemical sales/storage/transportation points in the surrounding area.

- Purchase or theft of restricted or sensitive chemicals.

- Rental of self-storage units and observed delivery of chemicals (possibly including explosives) to such units.

- Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units. (Also applies to explosives and incendiaries.)

- Chemical burns or missing hands and/or fingers treated at area hospitals or by area physicians. (Also applies to explosives and incendiaries.)

Biological Agent Indicators

- Sales or thefts of large quantities of baby formula or an unexplained shortage of it (the formula can be used as a medium for the growth of biological agents).

- Break-ins or tampering at water treatment or food processing/warehouse facilities.

- Solicitation for sale or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities.

- Persons stopped or arrested for possession of unexplained lethal amounts of disease agents or toxins.

- Multiple cases of unexplained human or animal illnesses or fatalities in the surrounding area, especially illnesses not native to the region.

- Sales (to nonagricultural users) or thefts of agricultural sprayers or crop-dusting aircraft, foggers, river craft (if applicable), or other dispensing systems. These can be used to spread biological agents. (Also applies to chemical and radiological agents.)

- Inappropriate inquiries regarding local or regional biological material sales, storage, or transportation points.

- Inappropriate inquiries regarding HVAC systems for buildings/facilities by persons not associated with organizations that service these systems. These systems can be used to spread a biological agent throughout a facility. (Also applies to chemical and radiological agents.)

Radiological Agent Indicators

- Break-ins or tampering at facilities that store radioactive materials or radioactive wastes.

- Solicitation for sale or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities.

- Persons stopped or arrested with unexplained possession of radioactive materials.

- Unexplained cases of human or animal radiation burns or radiation sickness or fatalities.

- Inappropriate inquiries regarding local or regional radioactive material sales, storage, or transportation points.

- Thefts, sales, or reported seizures of sophisticated personal protective equipment, such as "A"-level protective clothing, self-contained breathing apparatus (SCBA), etc. (Also applies to chemical and biological agents.)

- Thefts or sales of sophisticated filtering, air-scrubbing, or containment equipment. (Also applies to chemical and biological agents.)

COMMON VULNERABILITIES

Key Vulnerabilities

The following is a description of the key common vulnerabilities of religious facilities. In addition to the vulnerabilities specific to religious facilities, a number of general vulnerabilities can be identified that exist at many different infrastructure segments. These are provided in the reference section (DHS 2006).

- *Gathering of people of a particular faith.* A religious facility attracts a number of people of like faith into a single location at specified times. This makes the facility a ready target for an adversary seeking to attack that particular group of people.

- *Unrestricted access to religious services.* In general, religious facilities are open to all, at least during the conduct of religious services. Depending on the type of structure, the nature of access restrictions, and other security measures that may be in place, religious facilities may or may not be able to control access to the facility by potential adversaries. Some high-risk facilities employ private security guards and/or local police to assist in access control.

- *Unrestricted access to peripheral areas.* Religious facilities are vulnerable to attacks outside their main building, such as in contiguous parking areas, where vehicles have unrestricted access and are generally not inspected, and in auxiliary buildings such as educational facilities.

- *Building systems.* Buildings housing religious facilities have vulnerabilities similar to those of other buildings. Such vulnerabilities include explosions, fire, contamination via heating and cooling systems, and blocked emergency exits.

- *Access by workers and maintenance staff.* Workers and volunteers may not undergo background checks.

- *Easy identification.* Most religious facilities are readily identifiable either by their configuration or by signs.

- *Limited resources for security.* Most religious facilities are nonprofit. Many have very small budgets that are used to pay for the basic operation of the facility and to provide services to the congregation and surrounding communities. Many do not have the financial resources to implement extensive security measures.

Previous Incidents

A number of attacks have been made on religious facilities in the United States. Historically, these attacks have been racially motivated and/or driven by an interest in attacking the specific religious community that uses the facility. Depending on the definition used, these attacks may or may not be considered terrorist incidents.

In 1996, the National Church Arson Task Force (NCATF) was created in response to a large increase in the number of arson attacks on churches, primarily those with African-American congregations. The NCATF involves the Bureau of Alcohol, Tobacco, and Firearms; the Federal Bureau of Investigation; the Department of Justice; the Federal Emergency Management Agency; and the Department of Housing and Urban Development. In the latest report available, the NCATF reported opening 945 investigations of church arson, bombings, and threatened bombings between January 1, 1995, and August 15, 2000 (NCATF 2000).

The National Coalition for Burned Churches Research Center has documented approximately 685 arsons, bombings, attempted arsons, and fires of suspicious or undetermined origin over the three-year period from 1999 to 2001.

There have been numerous attacks on religious facilities and groups in other countries, including the following.

- In 1986, the Abu Nidal organization launched a major attack on the Neve Shalom Synagogue in Istanbul.
- In February 1994, the Kahane Chai (Kach) terrorist group supported Dr. Baruch Goldstein's attack on the al-Ibrahimi Mosque.
- In late 1994, Al-Qaeda's plan to assassinate Pope John Paul II during a visit to Manila was disrupted or not carried out.
- In the mid-1990s, 'Asbat al-Ansar' (a group associated with Osama Bin Laden) assassinated Lebanese religious leaders.
- Prior to 1996 in South Africa, the People against Gangsterism and Drugs (PAGAD) conducted bombing attacks on synagogues and moderate Muslims.
- In July 1997, the Loyalist Volunteer Force (LVF) in Northern Ireland murdered numerous Catholic civilians, including an 18-year-old Catholic girl because she had a Protestant boyfriend.
- In the months before January 2002, the Ulster Defense Association/Ulster Freedom Fighters (UDA/UFF) carried out more than 300 bombings and shootings against Catholics in Belfast.

- On April 11, 2002, Al-Qaeda carried out a firebombing of a synagogue in Tunisia.

- On August 5 and 9, 2002, the Pakistan extremist group Lashkar-e-Jhangvi conducted attacks on the Muree Christian School and Taxila Christian Hospital in which 10 people were killed and dozens injured.

- In the United Kingdom:

  - In 1999, the latest year for which figures are available, 462 church workers, including ministers and priests, were injured in attacks. And because many crimes are not reported, the figure is recognized by the British government as greatly understating the actual level of violence against church workers.

  - At the same time, a sample survey by researchers at London University found that 12% of Anglican clergy in England — about 1,300 priests — were attacked in 2000.

Consequences of an Event

The consequences of a successful attack on religious facilities can be wide-ranging. Consequences include the following.

Public Health and Safety Consequences

A terrorist attack against a religious facility could inflict a large number of casualties, particularly if conducted when there is a large congregation at a service. An arson attack; bombing; or the release of a biological, chemical, or radiological agent could create immediate casualties. A stampede toward the exits could add to the initial casualties. In the past, stampedes by crowds in buildings have killed and injured scores of people, sometimes more than are killed or injured during the precipitating event. Structural collapse could result from some types of attacks and add to the casualty list.

In addition to the immediate effects of an attack on a religious institution, there would be impacts on local, and perhaps regional, emergency service and public health resources. If a large religious facility were attacked, emergency response plans might need to be implemented. Multiple fire and rescue, hazardous material, law enforcement, and medical personnel, facilities, and equipment might need to be activated. Depending on its severity, an incident could tax available resources — a situation not unlike what would occur during a natural or accidental event such as an earthquake, tornado, hurricane, or fire.

Economic Consequences

Economic impacts could occur locally and perhaps regionally if a major religious institution were destroyed or incapacitated. Some religious facilities and their congregations participate heavily in the local economy.

Social and Institutional Consequences

The most significant consequence of an attack on a religious facility is the social and psychological effects on the congregation. These types of attacks are intended to instill fear into the targeted group of people. In some past instances of arson attacks on churches in the United States, community outrage at the attack has resulted in the dual reactions of fear on the part of the congregation and social unrest that has escalated into retaliatory attacks. Creating this type of social instability is one of the objectives of attacks on religious facilities.

Many religious facilities have active social programs, such as providing services to the poor, tutoring disadvantaged students, and assisting the elderly. An attack on a religious facility could disrupt these services.

Standards and Regulations

Like other institutional and commercial buildings, religious facilities are vulnerable to natural events (e.g., tornados, hurricanes, earthquakes), accidental events (e.g., structural collapse, utility system failures), and intentional events such as terrorist attacks. Building codes and construction standards have been designed and adopted to address natural and accidental events. Some of these codes and standards are also applicable to terrorist threats.

The International Code Council (ICC) is a nonprofit organization dedicated to developing a single set of comprehensive and coordinated national model construction codes. The ICC was founded by Building Officials and Code Administrators International, International Conference of Building Officials, and Southern Building Code Congress International. These nonprofit organizations developed three separate sets of model codes that were used throughout the United States. In 1994, these groups combined to form the ICC and develop a single set of codes without regional limitations. The ICC publishes a variety of references to building codes and standards, including the International Building Code and state and local codes. It offers technical publications that cover most topics associated with building structures. It also performs technical evaluations of building plans and provides technical support to its members. The ICC Web site provides links to the organization's publications and services.

In addition to the model codes, various jurisdictions, cities, and states amend the models or write their own codes to suit their own conditions. In 1967, the nation's governors founded the National Conference of States on Building Codes and Standards to promote the development of an efficient, cooperative system of building regulations to ensure the health, safety, and welfare of the public within the built environment.

The Federal Emergency Management Agency (FEMA) has published a series of risk management manuals and primers to help develop and enhance building terrorism resistance methodologies. According to FEMA, the *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*

> "…provides guidance to the building science community of architects and engineers, to reduce physical damage to buildings, related infrastructure, and people caused by terrorist assaults. The manual presents incremental approaches that can be implemented over time to decrease the vulnerability of buildings to terrorist threats. Many of the recommendations can be implemented quickly and cost-effectively."

FEMA states that the *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks* "introduces a series of concepts that can help building designers, owners, and state and local governments mitigate the threat of hazards resulting from terrorist attacks on new buildings." These relatively new publications are available online.

The United Kingdom's Home Office has produced a detailed publication entitled *Bombs: Protecting People and Property — A Handbook for Managers*. It was, according to its preface, "written specifically with managers in mind. The advice which it contains is relevant to all businesses and organizations…. It does not — cannot — address the particular circumstances of each reader." The fourth and latest edition of the handbook is available online in two parts.

The Centers for Disease Control and Prevention, in conjunction with the National Institute for Occupational Safety and Health, has issued a comprehensive report entitled, *CDC-NIOSH Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*. It details preventive steps that can be taken to reduce the likelihood of and mitigate the impact of threats and potential hazards associated with chemical, biological, or radiological terrorism. Although this document discusses buildings in general, many of the vulnerabilities and recommendations are applicable to religious facilities. The document is available online.

Many vulnerability studies with suggested remedies have been published that deal with potential incidents, not specifically terrorism-related, but with similar scenarios and consequences. Vulnerability to a fire and mitigation of the effects is one example. There are obvious differences in preventive measures; however, once a fire occurs (regardless of whether the cause was a gas line leak, faulty wiring, or arson attack), facility vulnerabilities are the same. The same is true of safety measures such as sprinkler systems and fire doors. The National Fire Protection Association (NFPA) has produced many publications and reports relating to fire prevention, including codes and standards, preventive measures, and alarm and signaling systems. Links to these documents can be found at the NFPA Web site.

Some religious organizations have published their own guidelines for facilities (e.g., Jewish Community Relations Council of New York). These provide general recommendations for how a religious facility might take steps to increase its security.

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, 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 2 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 the implementation of protective measures.

Table 2 DHS Advisory System Alert Levels

Alert Level		Description
Red	SEVERE	Severe risk of terrorist attack
Orange	HIGH	High risk of terrorist attack
Yellow	ELEVATED	Significant risk of terrorist attack
Blue	GUARDED	General risk of terrorist attack
Green	LOW	Low risk of terrorist attack

The measures shown on the following charts are designed to provide information and assistance to facility owners, site managers, local law enforcement, 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 steps taken in planning and preparing for emergencies.

- Designate an employee as security director to develop, implement, and coordinate all security-related activities.
- Conduct threat analyses, vulnerability assessments, and security audits on a regular and continuing basis. On the basis of these analyses, develop a comprehensive security plan and emergency response plan for the religious facility. Include the following:
  - Standard operating procedures (SOPs) to cover all potential emergency situations, including procedures for dealing with multiple events (e.g., explosives attack and loss of electric power).
  - Identification of security responsibilities and a chain-of-command for responding to an incident.
  - Operations Security (OPSEC) procedures to cover routine security activities by all employees.
  - Procedures for dealing with people who have special needs (e.g., with physical disabilities, non-English-speaking).
- Involve employees at several levels in security planning. Consider third-party evaluation and verification of the plans.
- Establish liaison and regular communication with local law enforcement and emergency responders, state and federal law enforcement and terrorism agencies, public health organizations, and industry organizations to enhance information exchange, clarify emergency responses, track threat conditions, and support investigations. Religious facilities' security and emergency response plans should be coordinated with appropriate agencies and should include mutual aid agreements. Critical information about the facility (e.g., floor plans, location of emergency equipment, notification and contact lists) should be shared with local law enforcement and emergency responders.
- Keep copies of the security and emergency response plans in redundant locations. Ensure that the plans are protected from unauthorized disclosure.
- Restrict access to sensitive facility data and information (e.g., facility building plans; mechanical, electrical, fire, and life safety systems).
- Ensure that one or more facility employees who are familiar with the plans are available for deployment at all times. Maintain lists of persons to contact in an emergency.
- Conduct regular exercises with facility employees to test the security and emergency response plans and to ensure that adequate resources are available to implement the plans. Also conduct regular exercises with law enforcement and emergency responders to familiarize them with the facility and its security and emergency procedures.
- Establish the capability to collect and interpret available threat intelligence from local, state, and federal agencies. Maintain constant awareness of current threat conditions and available intelligence information. As part of the security plan, establish procedures to implement additional protective measures as the threat level increases. Also establish procedures for returning to lower security levels as the threat decreases. Alert local law enforcement and emergency responders of measures being implemented.
- Keep records of all security-related incidents; review the records to identify patterns and trends.
- Develop policies and procedures for dealing with hoaxes and false alarms so that they would not unduly burden facility operations.

PLANNING AND PREPAREDNESS (Cont.)
These measures relate to steps taken in planning and preparing for emergencies.

- 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 diffuse rumors and panic.
- Establish procedures for facility evacuation and for shelter-in-place situations. Ensure that a facility is available for shelter-in-place situations that is adequately stocked with food, water, and supplies and that can accommodate the number of people who might need to use it.
- Consider installation of an emergency operations center or emergency command center that can be used to coordinate resources during an incident.
- Develop procedures for shutting down the facility in the event that the threat is deemed too serious to continue operations.
- Control all sensitive documents by requiring employees to secure them when not in use. Utilize shredders or a document service to destroy unneeded documents.

During Periods of High Alert (HSAS ORANGE)

- Review and implement actions specified in the security and emergency response plans; adjust them as necessary to address specific threat information.
- Activate facility emergency operations center as appropriate.

During Periods of Severe Alert (HSAS RED)

- Review available threat information and determine whether the facility should be closed or should operate with reduced hours, a reduced work force, 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 that can be used to reject an individual.
- Incorporate security awareness and appropriate response procedures for security situations into employee training programs. Include the following in the training:
  - SOPs in the security and emergency response plans that are to be used for different types of incidents
  - Maintaining alertness to and recognizing situations that may pose a security threat (e.g., suspicious persons, persons without proper employee identification, persons carrying unusual packages, unattended vehicles and packages, strange odors or liquids)
  - Contact and notification protocols for suspicious situations and emergencies
  - Caution in providing facility information to outsiders
  - Procedures to provide for the safety of employees during a security incident
- Maintain up-to-date security training with regular refresher courses. Maintain records of employee training that has been completed.
- Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., working irregular hours, attempting to access restricted areas, carrying unusual packages). Maintain awareness of any unusual patterns of employee illness that might indicate exposure to a toxic agent.
- Review the personnel files of recently terminated employees to determine whether they pose a security risk. Take appropriate actions to mitigate the risk.

Security Force

- Maintain an adequately sized, equipped, and trained security force that includes both employees and congregation volunteers. Ensure that adequate security personnel are on duty or on call in the event of an incident. Determine the availability of security force reinforcements that would be deployed during heightened threat conditions. Conduct more rigorous background checks on security force personnel.
- Develop a procedure and location for detaining and questioning persons displaying suspicious behavior and/or violating security regulations. Train security force in appropriate methods for handling these people.
- Conduct regular drills and exercises with security force. Involve local law enforcement and other agencies as appropriate.
- Develop a security force patrol schedule that includes both regular and random patrols.

PERSONNEL (Cont.)
These measures relate to personnel.

Contractors, Vendors, Temporary Employees, Visitors, Patrons

- Provide security information and training to all nonemployees visiting the facility. Advise them to be alert to suspicious activity or items and instruct them on how to report such 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 training and reminders to employees about the security situation. Provide refreshers on SOPs to be used for different types of incidents.
- Increase security force presence with overtime and/or additional personnel. Increase frequency of patrols.
- Consider augmenting the security force with armed guards and/or additional equipment.
- Extend patrols to a wider perimeter around the facility in coordination with local law enforcement.
- Have employees vary their routines to avoid predictability.
- Limit noncritical travel and business activity outside the facility.

During Periods of Severe Alert (HSAS RED)

- Increase security force presence to maximum level sustainable.
- Request additional security force support from law enforcement.

ACCESS CONTROL
These measures relate to steps taken in controlling access to the facility.

General Measures

- Define the facility perimeter and identify sensitive or critical areas within the facility (e.g., HVAC control rooms, mail rooms, fuel storage tanks, utility service areas) that require special access control for pedestrians and/or vehicles. Maintain the minimum number of facility access points needed to meet facility operational requirements and safety considerations. Where necessary, design layered access points that provide multiple opportunities to permit or deny entry. Where possible, locate sensitive equipment and assets in the interior of the facility. Evaluate and select access control measures for each access point.
- Provide appropriate signage to identify access points and areas with restricted access.
- Prohibit entry of security-sensitive items (e.g., firearms, explosives, illegal drugs). Train security force to identify and confiscate such items.
- Strictly enforce all access control measures (e.g., locking of buildings not in use) on a continuing basis; allow no exceptions.

Employees

- Issue photo ID badges to all employees. Require that badges be displayed and verified to gain access to the facility. Occasionally test the response of employees to unbadged persons at the facility.
- Collect employee ID badge and keys when employment is terminated. Consider changing locks.

Contractors, Vendors, Temporary Employees

- Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees. Require that the badges be displayed and verified to gain access to the facility. Require that badges be worn at all times in the facility. Collect all badges when visit is complete.
- Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement. Require sign-in and sign-out of contractors, vendors, and temporary employees.
- Encourage employees to develop a familiarity with contractors, vendors, and temporary employees. Have them question any unusual or unrecognized people and report incidents to facility security personnel.
- Escort all nonemployees when they are in sensitive or critical areas.

Congregation Members, Visitors

- Review all requests for tours, demonstrations, and displays (e.g., open house). If possible, discuss visitor requests with local law enforcement to identify potential problems.
- Require sign-in/sign-out for visitors. Issue special identification badges to visitors. Require that badges be displayed and verified to gain access to the facility. Require that badges be worn at all times in the facility. Collect all badges when visit is complete.

ACCESS CONTROL (Cont.)
These measures relate to steps taken in controlling access to the facility.

- Limit access by congregation members and visitors to a level consistent with facility operations. Train security personnel to deny access to anyone exhibiting suspicious behavior.
- Where possible, maintain a list of congregation members and other regular visitors.

Vehicles

- Consider using centralized parking and shuttle services to keep vehicles away from critical assets.
- Maintain a database of employee-owned vehicles; issue parking permits for designated areas.
- Positively identify all vehicles and drivers that enter the facility. Maintain a log of all nonemployee vehicles entering the facility. Deny access to suspicious vehicles (e.g., with leaking fluids, apparently heavily overloaded, with unusual odors) and to vehicles and drivers with improper documentation or refusing to provide identification and/or submit to inspection.
- Review vehicle traffic patterns. To the extent possible, keep vehicles away from sensitive or critical assets and from areas where large numbers of people congregate.
- Limit vehicle access to sensitive or critical areas to those with a definite need to be in the area, those that have been positively identified, and those that have been inspected.
- Lock all facility vehicles and park them in a secure area when they are not in use.
- Approach all illegally parked vehicles; require that they be moved or have them towed.

Buildings, Rooms, Shipping/Receiving Areas, Storage Facilities, Utility Access

- Provide adequate door and window locks, barred entryways, fencing and gate locks, timed closure devices, and other access controls to buildings, rooms, elevators, shipping/receiving areas, storage tanks and bins, utility access points (e.g., manholes, HVAC systems), hazardous materials (e.g., fuels, chemicals) storage areas, and other areas where access is to be limited. Add intrusion detection systems and alarms as appropriate. Employ more stringent security controls (e.g., card swipe locks, biometric identification) in sensitive or critical areas. Maintain an audit trail of people accessing these areas.
- Regularly inspect and test all access control devices.
- Provide additional security for buildings and other assets that are located along the facility perimeter and may be more open to attempts at unauthorized entry.
- Provide access control measures for ladders, awnings, and parapets that allow access to building roofs, HVAC systems, and other critical equipment. Ensure that nearby foliage (e.g., trees, shrubs) cannot be used to gain access to the roofs of buildings.
- Lock and secure all buildings and other assets when not in use. Ensure that all areas containing equipment used by the security force (e.g., communications gear, uniforms, weapons) are locked and secured.
- Implement rigorous key control procedures. Track holders of all keys. Secure master keys. Require that terminated employees and contractors who have completed their work return all keys.

ACCESS CONTROL (Cont.)
These measures relate to steps taken in controlling access to the facility.

- Secure all tools that could be used to force entry into a secured area, building, or room (e.g., bolt cutters, hacksaws).

Mail, Shipments, Deliveries

- Train mail room and receiving personnel to recognize suspicious mail, packages, shipments, or deliveries and instruct them in the procedures to follow.
- Accept deliveries and shipments only from known shippers, vendors, or customers.

During Periods of High Alert (HSAS ORANGE)

- Reduce the number of access points for pedestrians and vehicles. Increase the security (e.g., additional guards, inspections) at each open access point.
- Restrict access by nonemployees (e.g., contractors, vendors, visitors) to those needed to support critical activities. Delay nonessential contractor work. Escort all nonemployees while at the facility.
- Restrict parking to areas away from critical assets. Evaluate the closure of underground or under-building parking lots.
- Consult with local authorities about restricting access to the buffer zone around the facility. Evaluate the need for closing or restricting traffic on nearby roads, waterways, or public access areas adjacent to the facility. Implement measures as appropriate.
- Redirect mail, shipments, and deliveries to areas distant from sensitive or critical assets. Accept deliveries only during daytime hours.

During Periods of Severe Alert (HSAS RED)

- Consider closing facility until threat has been reduced.

If the decision is made to keep the facility open:

- Reduce access to an absolute minimum.
- Allow no access to nonemployees. Halt all contractor work. Allow no visitors.
- Accept no nonessential mail, shipments, or deliveries.

BARRIERS
These measures relate to physical barriers and barricades.

Facility Perimeter Barriers

- Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility. Consider natural features (e.g., hills, woods, waterways) that could either enhance or inhibit security at the facility. Consider delay time created by barriers and evaluate for adequacy.
- Install appropriate perimeter barriers and gates. Implement appropriate level of barrier security (e.g., chain-link fencing, barbed-wire fencing, electrified fencing, chained gates, remotely closed gates). Remove trees, vegetation, or other obstructions along perimeter barriers to enable continuous monitoring and to inhibit concealment of people or packages. Inspect perimeter barriers regularly.
- Install alarms and intrusion detection equipment at perimeter barriers.

Building Barriers

- Establish a clear zone adjacent to sensitive or critical buildings. Keep zone free of vegetation and other obstructions to allow for continuous monitoring and to inhibit concealment of people or packages.
- If appropriate, install building perimeter barriers (e.g., fences, bollards, decorative flower pots, high curbs, shallow ditches) around sensitive or critical buildings in addition to the facility perimeter barriers. Consider the requirements for fire protection and emergency vehicle access in the design of building perimeter barriers.
- If appropriate, install interior building barriers (e.g., internal locked doors) to protect sensitive or critical areas or corridors within a building.
- Install barriers to protect doors and windows from small arms fire and explosive blast effects (e.g., blast-resistant and shatter-resistant glass, offset entryways, shrubbery).
- Ensure that buildings have smoke-proof stairways and exit corridors that can be used for evacuation.
- Ensure that exterior doors have hinge pins that cannot be removed from the outside and that there are no gaps between the door and jamb that would allow for the door to be compromised.
- Install barriers at HVAC systems (e.g., screens on intakes, filters) to prevent the introduction of chemical, biological, or radiological agents into buildings. Where needed, provide positive pressure in buildings to prevent contaminants from entering. Train staff in emergency shut-off procedures for HVAC systems.
- Move objects that could become projectiles (e.g., trash containers, crates, loose items not attached to a building or to the ground) a safe distance from buildings and areas where large numbers of people congregate.

Vehicle Barriers

- Evaluate vehicle traffic patterns at the facility. Design and implement traffic control strategies and barriers (e.g., road alignment, serpentine traffic routing, retractable bollards, swing gates, speed bumps, tire shredders) to control vehicle speed and approaches to sensitive or critical assets.

BARRIERS (Cont.)
These measures relate to physical barriers and barricades.

- Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from buildings and areas where large numbers of people congregate.
- Install bollards on pedestrian walkways to keep vehicles off them.

During Periods of High Alert (HSAS ORANGE)

- Inspect all barriers and repair as needed.
- Deploy temporary barriers (e.g., Jersey barriers, heavy vehicles and equipment, empty containers, trucks loaded with sand) to increase the standoff distances from the facility and buildings.
- Deploy temporary barriers to slow the flow of traffic into the facility grounds and within the facility.
- Relocate sensitive or critical items (e.g., specialized equipment, important records) to areas of the facility with greater physical security.

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.

General Measures

- Develop a communication and notification plan that covers voice, data, and video transfer of information related to security.

Communications Equipment

- Install system(s) that provide communication with all people at the facility, including employees, security force personnel, and congregation members, and visitors. Provide redundant communication channels (e.g., telephone, radio, pager, public address system) that can be used in the event that one channel is disabled. Provide backup electric power (e.g., backup generators, uninterruptible power supplies) to run communications equipment. Consider installation of special "panic alarm" systems in sensitive or critical areas. Consider installation of a priority access communication system to allow preferred access to users involved in emergency management. Test systems regularly. Train employees in the use of the various communications systems.
- Install system(s) that provide communication channels with local law enforcement and emergency responders. Provide redundant communication channels and backup power. Test systems regularly.
- Have emergency communication equipment (e.g., special cell phones, emergency radios) available for use in the event that all primary communication channels are unavailable.
- Provide communication security (e.g., encryption, multiple frequencies) that will prevent unauthorized interception of information being transferred. Regularly conduct countermeasures sweeps of the communications systems to uncover any eavesdropping or other security compromises. Train employees not to discuss sensitive information over communications channels that are not secure (e.g., cell phones).
- Provide the ability to record incoming communications (e.g., telephone calls) to identify potential threats.
- Confirm interoperability of communication systems between facility organizations and with local emergency responders. Ensure that all parties can communicate with each other.
- Coordinate with communication service providers (e.g., telecommunications companies) on plans and procedures for restoration of service in the event of a disruption.

Communication Protocols

- Develop a notification protocol that outlines who should be contacted in emergencies. Designate who is to contact whom within the facility and with outside organizations. Provide a contact list to all who might need it and keep the list up to date. Regularly test 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., a hot line number, internal 9-1-1 capability).

COMMUNICATION AND NOTIFICATION (Cont.)
These measures relate to communications.

- Develop a process for communicating to employees the current security situation and reminding them of steps that should be taken in the event of an incident. Keep security advisories up to date as the situation changes. Develop a process for communicating with employees who are not on duty.
- Establish call-in procedures for employees who are away from the facility or who work in remote or isolated locations. Utilize these procedures for both routine and emergency situations.
- Develop a process for communicating with the public and the media regarding security issues. Identify the people who will have responsibility for media interactions. Provide adequate information to quell rumors and prevent unnecessary alarm. Take steps to restrict the release of information that might compromise the security posture of the facility.

Information Sharing

- Monitor information on threats, incidents, and response procedures. As appropriate, share information about the facility's experiences.

During Periods of High Alert (HSAS ORANGE)

- Increase frequency of communications with local law enforcement. Advise them of the heightened security status of the facility. Identify additional security measures that will be implemented.
- Increase communication with employees about the security situation and provide reminders about actions to take in the event of an incident.
- Test communication equipment, including primary and backup systems, more frequently.

During Periods of Severe Alert (HSAS RED)

- Maintain communication with local law enforcement as continuously as is sustainable.
- Provide employees with as much information as possible as frequently as possible to keep them apprised of security situation.
- Have communication backup equipment activated and 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 in and around a facility.

General Measures

- Evaluate needs and design a monitoring, surveillance, and inspection program that is consistent with facility operations and security requirements. Coordinate with local law enforcement on activities to be undertaken, particularly with regard to monitoring the area surrounding the facility. If appropriate, enlist local community groups (e.g., block or neighborhood watch groups) to help provide security-related monitoring in the surrounding area.

Equipment

- Provide visual surveillance capability (e.g., designated surveillance points, observation towers, cleared lines of sight) for sensitive and critical assets at the facility. Assign and train personnel, including security force and other employees, to maintain vigilance to unusual activities in sensitive or critical areas. Keep surveillance areas clear of obstructions (e.g., vegetation, parked vehicles) that would inhibit observation.

- Install video surveillance equipment (e.g., closed-circuit television [CCTV], lighting, night vision equipment). Provide coverage for the perimeter, sensitive and critical assets in the facility, vehicle roadways and parking lots, and building entrances. Include coverage of the buffer zone around the facility. Provide both centralized and distributed capability to monitor and record video feeds. Maximize video recording time. Train personnel to interpret video and identify potential security-related events. Review recordings regularly for unusual activities or patterns. Establish procedures to secure video recordings for forensic purposes. If appropriate, provide video feed to local law enforcement and/or to other organizations outside the facility. Inspect and test all video equipment regularly.

- Install detector and alarm systems. Include intrusion detectors, fire and smoke alarms, motion detectors, chemical/biological/radiological material detectors, and explosives detectors as appropriate. Provide both centralized and distributed capability to monitor and record detector and alarm feeds. Maximize the recording time. Train personnel to interpret detector and alarm signals and to identify potential security-related events. Review recordings regularly for unusual activities or patterns. Establish procedures to secure detector and alarm recordings for forensic purposes. If appropriate, provide detector and alarm feed to local law enforcement and/or to other organizations outside the facility. Inspect and test all equipment regularly.

Buildings and Facility Assets

- Deploy security force to regularly inspect facility perimeter, buildings, parking lots, locker rooms, equipment, trash containers, HVAC systems, and sensitive or critical areas for signs of security issues or breaches. Ensure that security force has access to all areas to be inspected. Implement random, as well as scheduled, inspections. Utilize plain-clothes, as well as uniformed, patrols. Employ vehicle, foot, and bicycle patrols as appropriate. Pay special attention to assets that are not in frequent use. Train security force and other employees about items they must be alert to and instruct them on reporting procedures.

MONITORING, SURVEILLANCE, INSPECTION (Cont.)
These measures relate to procedures and equipment used to monitor the movements of people, vehicles, and materials in and around a facility.

People

- Continuously monitor all people entering and leaving the facility. Train monitors to detect suspicious behavior (e.g., unusually bulky clothing that might conceal weapons, unusual packages being carried).
- Inspect packages, briefcases, backpacks, parcels, and luggage carried by congregation members, employees, contractors, vendors, and visitors. Inspection may be spot check or comprehensive.
- Monitor the activities of contractors, delivery personnel, and vendors while they are at the facility for unusual behavior.

Vehicles

- Continuously monitor all vehicles approaching the facility for signs of threatening behavior (e.g., unusually high speed, approaching restricted areas). Be prepared to take defensive action against vehicles exhibiting such behavior (e.g., engage barriers, deploy security force vehicles).

Deliveries and Mail

- Inspect all deliveries made to the facility. Supervise the unloading of materials and equipment. Verify the shipper, driver, delivery manifest, and material being unloaded to ensure conformity to expected deliveries. Verify that seals on deliveries have not been tampered with. Conduct more thorough inspections for deliveries involving hazardous or sensitive materials. Reject any deliveries that fail to conform to requirements.
- Maintain records of all deliveries (e.g., bills of lading, invoices).
- Inspect all mail for unusual characteristics (e.g., strange powders, leaking material, no return address). Divert to controlled area for handling. Provide personal protective equipment for those handling suspicious mail or packages.
- Advise employees to check all deliveries and mail at home for suspicious material.

Materials

- Maintain a thorough inventory and accounting of all sensitive or critical materials and equipment and their storage and movement into, out of, and within the facility.
- Monitor contractor work done at the facility (e.g., construction, equipment installation, maintenance, cleaning) for unusual activities. Inspect all work before releasing the contractor.
- Monitor work being done adjacent to the facility (e.g., road construction, utility equipment servicing) for unusual activities (e.g., someone photographing the facility or planting packages near facility perimeter or assets).

MONITORING, SURVEILLANCE, INSPECTION (Cont.)
These measures relate to procedures and equipment used to monitor the movements of people, vehicles, and materials in and around a facility.

During Periods of High Alert (HSAS ORANGE)

- Increase monitoring, surveillance, and inspection of sensitive and critical assets, people, vehicles, materials, and equipment. Reassign staff to assist with surveillance, monitoring, and inspection duties.
- Increase monitoring of video surveillance, alarms, and detector equipment feeds. Route detector feeds to local law enforcement.
- Install additional temporary lighting to illuminate all areas. Leave lighting on 24 hours. If possible, increase lighting in buffer zone.
- Restrict what people are permitted to carry into the facility.
- Deploy portable scanning equipment (e.g., metal detectors, x-ray scanners) to increase the level of inspection.
- Isolate or remove any hazardous materials that might increase the impacts of an attack.

During Periods of Severe Alert (HSAS RED)

- Increase staff assigned to surveillance, monitoring, and inspection duties to a maximum sustainable level. Request additional support from local law enforcement.
- Implement continuous monitoring of video surveillance, alarms, and intrusion detection feeds.
- Increase frequency and thoroughness of inspections of buildings and facility assets to the maximum level sustainable. Close and secure nonessential buildings and assets.
- Thoroughly inspect all mail and deliveries made to the facility. Postpone all nonessential deliveries. Process mail and deliveries at a remote site.

CYBER SECURITY
These measures relate to steps taken in protecting information and computer systems.

- Develop and implement a security plan for computer and information systems hardware and software. Design and implement a secure computer network architecture.
- Develop a recovery and restoration plan to return computer systems to full functionality after an incident. Evaluate the feasibility of manually relocating essential computer equipment in the event of an incident. Identify sources for replacement equipment that could be brought into service quickly.
- Regularly test computer security measures (e.g., audits, penetration testing).
- Maintain complete documentation of computer system hardware and software modifications. Require a formal change management process to track all modifications.
- Maintain a well-trained computer security staff with the appropriate knowledge and experience to deal with cyber security issues. Conduct more thorough background checks on employees serving as system administrators.
- Carefully validate the credentials of all contractors and vendors given access to computer systems. Monitor and review their work when completed.
- Provide training to all employees using facility computer systems on cyber security threats (e.g., e-mail phishing, deceptive inquiries from outsiders, malicious code [e.g., viruses, worms, Trojan horses]), measures they can utilize to protect the system, and their cyber security responsibilities (e.g., changing passwords regularly, not divulging computer information to others, not opening unknown email attachments). Immediately cancel computer access for terminated employees.
- Install and maintain up-to-date cyber security techniques (e.g., firewalls, virus protection, spyware protection, encryption, user authentication) and software patches. Monitor computer systems regularly to detect any patterns of probing, hacking, or intrusions. Work with Internet service provider to implement protective measures against attacks (e.g., denial-of-service attacks). Stay up to date on the latest cyber security threats, incidents, and defensive measures.
- Control physical access to information technology (IT) facilities (e.g., computer rooms, SCADA control systems). Install locks and access controls to allow only authorized personnel to enter these facilities. Provide communication capabilities to allow rapid reporting of incidents.
- Control both on-site and off-site electronic access to IT systems by employing passwords, account access restrictions, and other control techniques.
- Develop redundancy in computer hardware and software to permit continued operation of information systems in the event that primary systems are disabled. Back up computer files regularly. Maintain backups in a separate and secure location.
- Thoroughly test all applications that involve handling of sensitive information to determine their potential vulnerability to compromise.
- Regularly review facility Web site to ensure that no sensitive information is provided.

CYBER SECURITY (Cont.)
These measures relate to steps taken in protecting information and computer systems.

During Periods of High Alert (HSAS ORANGE)

- Delay scheduled maintenance and upgrades on software and hardware that is not security related.
- Increase frequency of system backups.
- Increase monitoring for system probes, intrusions, and other anomalies. Advise employees to increase vigilance to unusual computer activities.
- Reduce access to the Internet and other portals that might present a security risk.
- Restrict instant messaging and peer-to-peer applications.
- Make technical support personnel available to deal with any problems.
- Delete information from the facility Web site that may help a potential adversary to plan an attack.

During Periods of Severe Alert (HSAS RED)

- Increase computer security to maximum levels.
- Reduce access to computer systems to the minimum level possible.
- Reduce access to the Internet and other portals to the absolute minimum needed to continue operations.
- Provide continuous monitoring of computer system for anomalies.
- Have technical support available on call 24/7.
- Consider disabling facility Web site.

INFRASTRUCTURE INTERDEPENDENCIES
These measures relate to the protection of utilities that support the facility, including electric power, natural gas, water, telecommunications, trash collection, and others.

- 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 company, gas company) to review existing systems, capacity expansion needs, and actions to be taken in response to loss of service from primary supply sources and other emergencies.
- As much as practical, locate utility supply facilities that are potentially hazardous (e.g., liquid fuel tanks, high-voltage power lines) a safe distance from buildings and areas where large numbers of people congregate.
- Ensure that employees are familiar with procedures for shutting 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. Install special locking devices on utility access points (e.g., manhole covers, HVAC vents).
- Provide for regular monitoring and inspection of utility services (e.g., security force patrols, CCTV) and their security measures.
- Where practical, 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 than the primary supply equipment. Inspect and maintain redundant and backup equipment regularly.
- Develop plans for decontamination (e.g., from chemical, biological, radiological agents) of infrastructure facilities.
- Secure dumpsters and other trash containers to prevent the hiding of explosives or other hazardous materials 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.
- 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 continuous security guard presence at critical utility points.

INCIDENT RESPONSE
These measures relate to steps taken in responding to an actual incident.

- Develop and maintain an up-to-date emergency response plan (see Planning and Preparedness).
- Ensure that an adequate number of emergency response personnel are on duty and/or on call at all times. Ensure that there are backup personnel who can execute emergency response functions in the event that primary personnel are unavailable or incapacitated. Ensure that adequate equipment and supplies are available to support emergency response requirements.
- Review unified incident command procedure for responding to an event with local law enforcement, emergency responders, and government agencies.
- Establish an emergency operations center or emergency command center that can be used to coordinate resources during an incident.
- Provide training and equipment to emergency response personnel to enable them to deal with terrorist-related incidents (e.g., chemical/biological/radiological agents, suicide bombers). Conduct regular 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.
- Check the status of all emergency response equipment and supplies on a regular basis. Store emergency supply kits in areas where they will be readily accessible to employees. Provide adequate security for emergency response equipment, facilities, and personnel. Do not leave emergency vehicles or equipment unattended or unsecured.
- Identify entry and exit points to be used in emergencies. Ensure that they are free of obstructions and can be fully utilized. Inspect these points regularly for signs of tampering and intentional obstruction. Train all employees on the location of these points.
- Identify alternate rallying points where employees and others at the facility can gather for coordinated evacuation and/or for “head counts” to ensure all have been evacuated. Identify alternate transportation routes for employees and others at the facility for use during evacuations. Test the routes by means of drills and exercises.
- Develop a list of key personnel who can be pre-approved to enter the facility after an incident and assist with recovery activities.
- Develop policies and procedures for dealing with the media and the general public in the event of an incident to apprise them of the situation and to diffuse rumors and panic.
- Establish procedures for facility evacuation and for shelter-in-place situations. For shelter-in-place situations, ensure that a facility is available that is adequately stocked with food, water, and supplies and that can accommodate the number of people who might need to use it.
- Develop plans to provide counseling to employees in the aftermath of an incident.
- Implement procedure for capturing lessons learned and developing revised response plans after an incident.

INCIDENT RESPONSE (Cont.)
These measures relate to steps taken in responding to an actual incident.

During Periods of High Alert (HSAS ORANGE)

- Review and implement actions specified in the emergency response plans; adjust as necessary to deal with specific incident conditions.
- Activate facility emergency operations center as appropriate.
- Pre-position emergency response personnel and equipment to locations that would enable rapid response to an incident.
- Review procedures with employees assigned to shut off utilities (e.g., electricity, water, natural gas) in the event of an incident.
- Prepare to execute contingency plans, such as moving personnel to an alternate location. Consider releasing all noncritical facility personnel.

During Periods of Severe Alert (HSAS RED)

- Review available threat information and determine whether the facility should be closed or should operate with reduced hours, a reduced work force, and/or reduced activities. Evaluate criteria for when facility should be reopened or restored to full operation.
- Bring emergency operations center up to full capability on a 24/7 basis.
- Cancel all leave and travel for facility personnel.

REFERENCE MATERIAL

Adherents.com [http://www.adherents.com/].

American Baptist Churches USA, "Mission Center Online" [www.abc-usa.org].

Association of Statisticians of American Religious Bodies, *Religious Congregations and Membership in the United States 2000*, published by Glenmary Research Center, North Nashville, TN [http://www.glenmary.org/grc/RCMS_2000/release.htm].

Baptist.Org, "Homepage for All Baptists" [www.baptist.org].

Catholic Online [www.catholic.org].

Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, 2002, *CDC-NIOSH Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, U.S. Department of Health and Human Services (NIOSH) Publication No. 2002-139, May [http://www.cdc.gov/niosh/bldvent/2002-139.html].

Chaves, M., 1998, *National Congregations Study*: *Data File and Codebook*, University of Arizona, Department of Sociology, Tucson, AZ [http://www.thearda.com/].

Christianity Today, 2001, "Church Attacks Increasing in the UK," Jan. 29 [http://www.christianitytoday.com/ct/2001/105/15.0.html].

Christianity Today, 2000, "'Missionary of Lucifer' Pleads Guilty to Church Burnings: Indiana Man Confesses to More Than 25 Acts of Arson," Dec. 6 [http://www.christianitytoday.com/ct/2000/149/35.0.html].

Church of Jesus Christ of Latter-day Saints, "Conference Center, Salt Lake City, Utah" [http://www.lds.org/placestovisit/location/0,10634,1867-1-1-1,00.html].

Federal Emergency Management Agency, 2003, *FEMA 426 — Reference Manual to Mitigate Potential Terrorist Attacks against Buildings,* Dec. [http://www.fema.gov/pdf/fima/fema426.pdf].

Federal Emergency Management Agency, 2003, *FEMA 427 — Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks,* Dec. [http://www.fema.gov/pdf/fima/fema427.pdf].

Federal Emergency Management Agency, 2003, *FEMA 429 — Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings,* Dec. [http://www.fema.gov/pdf/fima/fema429.pdf].

Houston's First Baptist Church [www.hfbc.org].

Lakewood Church [www.lakewood.cc].

International Code Council [http://www.iccsafe.org/].

Jewish Community Relations Council of New York, 2002, *Security Guide for Synagogues, Schools and Communal Institutions*, New York.

Kosman, B.A., E. Mayer, and A. Keysar, 2001, "American Religious Identification Survey" [http://www.gc.cuny.edu/faculty/research_studies/aris.pdf].

Mueller, R.S., III, 2003, "War on Terrorism," Statement for the Record by the Director of the Federal Bureau of Investigation before the Select Committee on Intelligence of the U.S. Senate, Washington, DC, Feb. [http://www.fas.org/irp/congress/2003_hr/021103mueller.html].

National Church Arson Task Force, 2000, *Fourth Year Report to the President*, U.S. Department of Justice, Washington, DC, Sept.

National Coalition of Burned Churches [www.ncfbc.org].

National Conference of States and Building Codes and Standards [http://www.ncsbcs.org/].

National Council of the Churches of Christ in the U.S., 1996 "NCCCUSA Board Calls Church Attacks 'A National Disaster,'" May 22 [http://www.wfn.org/1996/05/msg00781.html].

National Fire Protection Association, "NFPA Online" [http://www.nfpa.org/catalog/home/index.asp].

Pizam, A., and A. Fleischer, 2001, *Severity vs. Frequency of Acts of Terrorism: Which Has a Larger Impact on Tourism Demand?* Working Paper 20117, The Center for Agricultural Economic Research, Rehovot, Israel, Oct. [http://departments.agri.huji.ac.il/economics/pdf 20117.pdf].

Presbyterian Church (USA) [www.pcusa.org].

Southern Baptist Convention [www.sbc.net].

Texas Tech University Wind Science and Engineering Research Center, "Fujita Scale Enhancement Project Damage Indicators" [http://www.wind.ttu.edu/f_scale/indicators.htm].

Trinity Architecture & Planning, Inc., *Case Study for Second Baptist Church in Houston* [http://www.trinityarchitecture.com/].

United Kingdom Home Office, *Bombs: Protecting People and Property — A Handbook for Managers*, 4th ed. [http://www.ukresilience.info/contingencies/business/bombs.pdf].

United Methodist Church [www.umc.org].

U.S. Department of Homeland Security, 2004, *Terrorist Organization Reference Guide,* Bureau of Customs and Border Protection, U.S. Border Patrol, Jan.

U.S. Department of Homeland Security, 2006, *Overview of Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures for Critical Infrastructures and Key Resources,* Protective Security Coordination Division, Office of Infrastructure Protection.

OTHER USEFUL INFORMATION

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

The White House, 2003b, *The National Strategy to Secure Cyberspace*, Feb. [http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf].

The White House, 2003c, Homeland Security Presidential Directive/HSSPD-7, Dec.17, [http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html].

U.S. Department of Homeland Security

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

U.S. Department of Homeland Security, 2005, Interim National Infrastructure Protection Plan, Feb. [http://www.educause.edu/ir/library/pdf/CSD3754.pdf].

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/].

U.S. Air Force, Office of Special Investigations, *Eagle Eyes Program: Categories of Suspicious Activities* [http://public.afosi.amc.af.mil/eagle/suspicious_behavior.asp].

Other Organizations

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

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].

United Kingdom Home Office, *Bombs: Protecting People and Property — A Handbook for Managers*, 4th ed. [http://www.mipt.org/pdf/bombs_protectpeopleproperty.pdf].

DHS Reader Satisfaction Survey

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

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.

Circle your response accordingly:

1 Strongly Disagree
2 Disagree
3 Neither Agree or Disagree
4 Agree
5 Strongly Agree
NA Not Applicable

Quality

1 2 3 4 5	Information in this report is presented clearly and logically.
1 2 3 4 5	The content and documented sources make this report reputable.
1 2 3 4 5 NA	The LENS web site is easy to access.
1 2 3 4 5 NA	Information on the LENS web site is easy to navigate and find.

Value

1 2 3 4 5 NA	This report is relevant to your mission, programs, priorities, or initiatives.
1 2 3 4 5 NA	This report enhanced your knowledge of infrastructure protection.
1 2 3 4 5 NA	This report will likely result in changes to your existing protection practices.
1 2 3 4 5 NA	This report will likely result in more informed protection decisions.
1 2 3 4 5	I will recommend that colleagues review this report.

Comments

Title or type of report: _____Organization or reader name: _____