pick a lock, in most cases, entry is made using physical force by smashing doors, crow-barring doors or windows, and breaking window glass. Some burglars have resorted to breaking through building walls with sledgehammers. The risk of burglary is also influenced by the store's hours of operation. Those that operate 24 hours a day, 7 days a week are the least vulnerable to burglary.

A.16.4.3.2 Adequate outside lighting of the parking area and approaches during nighttime hours of operation enhances employee and customer protection.

A.16.4.5 Clear visibility into the premises enables passersby and police patrols to observe activities inside, which can serve as a deterrent to robbery. It also enables employees to observe suspicious activities outside.

A.16.5.3.2.1 Executing a burglary involves locating and collecting items of value. Factors that affect the time burglars will spend on the premises include the skill and confidence of the burglar(s), whether valuables are stored in a safe or vault, the quality of the protection, and the anticipated response by the police or designated personnel. An intrusion detection system can deter a burglar. An alarm system that sends a signal to a monitoring station that dispatches designated personnel on receipt of the signal is preferred. An alarm system that sounds a local bell is better than no alarm at all — at the very least, it might scare off the burglar.

A.17.1.1 Since there are many different types of shopping centers (e.g., enclosed malls, open-air centers, neighborhood centers, and strip malls), and their locations warrant different security measures, no single set of security measures can apply to all shopping centers.

A.17.1.2.1 Because shopping centers offer such a diversity of facilities, activities, and clientele, no single security program will fit all properties. The security program should be designed to fit the needs and characteristics of the individual property. While crime is not always preventable, certain policies and procedures, properly implemented, can deter or discourage criminal activity.

An effective security plan cannot stop all crime. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.17.1.3(3) The SVA can help determine the need for physical security measures, such as fencing, lighting, video surveillance, and access control systems.

A.17.1.3(4) Establishing and maintaining liaison with local law enforcement agencies will provide for the exchange of information concerning the level of criminal activity on the property and in the immediate neighborhood, as well as crime prevention services that are available. Establishing a positive relationship with law enforcement creates a partnership that is helpful in providing crime prevention services and information to the landlord and tenants. Information on criminal activity can be requested from local law enforcement where it is available and they have the ability to reproduce it.

A.17.1.3(5) Emergency policies and procedures are helpful when an emergency or disaster strikes. The purpose of having written policies and procedures is to provide a plan that can be used to minimize damage to property and prevent or reduce possible injury to employees and visitors. Emergencies can be caused by natural and man-[illegible] mechanical or equipment failure. The effects these emergencies can have on employees, customers, and visitors range from mild disruption to possible evacuation. Emergency procedures should be developed by utilizing information provided by government agencies, such as the Federal Emergency Management Agency (FEMA), and in cooperation with local public safety and emergency management agencies. A method of communicating important information to tenants is a part of any emergency plan.

A.17.2.1.2 One way to provide notification is by monthly newsletter.

A.17.2.1.3.1 Management will regularly review its security needs and provide personnel to respond to emergencies and assist customers and employees as required. If contract security is utilized, the security contractor is responsible for the selection, training, and supervision of personnel and for complying with all state and local laws, rules, and regulations.

A.17.2.1.3.3 Management should consider having some of their security personnel visible, in an effort to deter criminal activity. Security personnel should patrol the premises on a regular schedule, but not in a predetermined pattern. Patrol rounds should include exterior grounds, building perimeter, parking areas, stairwells, exit and delivery corridors, and storage, receiving, and trash disposal areas. The number of security personnel on patrol can vary by time of day, day of the week, and the season of the year, depending on local security problems, peak traffic periods, and special events.

A.17.3 Where circumstances warrant, consideration should be given to establishing perimeter security. Fencing or other physical barriers, if appropriate, at the perimeter of the protected asset can discourage unauthorized access to the protected asset and might deter the opportunistic criminal.

A.17.4 The security program for a shopping center often starts at the architect's desk. Every developer and architect must consider security requirements and potential security problems when designing a new shopping center or expanding or renovating an existing facility.

A.17.4.3 Lighting is basic to any security program. Local ordinances and building codes can mandate lighting requirements.

A.17.4.4 Landscaping serves the primary purpose of aesthetics but can also create security problems. For example, overgrown shrubbery can provide concealment, and trees planted too close to the fence line can serve as a means for scaling fences. Management should consider providing a clear zone between the tops of shrubbery and the bottom branches of the trees, for surveillance purposes.

A.17.5.3.3 If utilized, a video surveillance system can cover all entrances, exits, entrance ramps, elevators, stairwells, walkways, and parking areas. Lighting levels might have to be increased for proper operation of the video surveillance system. Signs stating that the area is under surveillance can serve a deterrent function. Fake cameras must never be used — they give a false sense of security. Video surveillance is a tool that can be used to record historical data that can assist the police in solving crimes.

A.17.6 Because of the significant risks they pose, parking facilities are to be afforded special consideration.

A.18.1.2.1 A security program for retail establishments should [illegible], robbery, burglary, shop-

lifting, fraud, and workplace violence. The security program should be designed to fit the needs and characteristics of the individual property. While crime is not always preventable, certain policies and procedures, properly implemented, can deter or discourage criminal activity.

An effective security plan cannot stop all crime. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.18.1.2.3 A retail establishment's hours of operation and the amount of cash on hand affect its risk of robbery. In general, any business with cash on the premises is a prospective target for robbers, even though the amount of cash on hand might not be high. As such, robbery prevention measures must be implemented to reduce the risk of robbery and the violence that can result from robbery.

A.18.2.1.1.2.2(1) Having at least two employees on duty during high-risk hours and at opening and closing times will serve as deterrents to robbery.

A.18.2.1.1.3 The key to reducing employee theft is for management to admit that theft is possible and then create an environment that makes stealing as difficult as possible. An analysis of the opportunities for theft within a company must be performed so that strategies can be developed to reduce or limit the exposure. In any event, the application of these procedures and devices must be performed with the knowledge and agreement of employees; otherwise, there can be a damaging effect on employee morale and productivity.

A.18.2.1.1.3(2) For example, the person who has the authority to write checks and make deposits cannot be responsible for reconciling the bank statement.

A.18.2.1.2.1 Shoplifting occurs when it is easy and convenient for the shoplifter. While it is impossible to eliminate shoplifting losses completely, it should be the goal of the retail establishment to deter the would-be shoplifter as much as possible through the proper use of people and equipment. A shoplifting prevention program generally consists of procedural controls and a policy of arrest and prosecution.

Procedural controls are intended to eliminate the opportunity for shoplifting. The physical layout of the store should be such that it discourages shoplifting. High value merchandise cannot be located near doors, and aisles should not be cluttered. Cash registers should be located so that customers have to pass by them to exit the store. The number of entrances and exits should be limited but not in violation of life safety and building codes. Customers are not allowed to use fire exits except in an emergency. Prevention methodologies, such as convex mirrors and video surveillance, should also be considered.

Generally, the most important element of a shoplifting prevention program is the arrest and prosecution of shoplifters who will not otherwise be deterred. Prosecution not only serves to impress upon the person arrested that shoplifting will not be tolerated by the store, but it establishes an attitude that becomes known in the community.

Because of ignorance of the law and fear of lawsuits, many retail businesses are reluctant to detain or arrest shoplifters. What begins as the apprehension of a suspected thief can be converted into grounds for a civil suit against the business owner if proper procedu[illegible] one (even momentarily) without hard evidence of theft can lead to a lawsuit for false arrest.

All states have laws called *merchant's privilege laws,* which are intended to protect stores from civil lawsuits and criminal charges arising from the detention and questioning of suspected shoplifters. These laws provide protection against suits for false arrest, provided the suspect has been detained in a reasonable manner and for a reasonable period of time and that there is reasonable assurance that the suspect has taken merchandise with no intention of paying for it.

A person is not necessarily guilty of shoplifting just because he or she did not pay for an item. It is not a crime to forget to pay for something. For a person to be guilty of shoplifting, it is necessary to prove that there was intent to steal. This requires that the shoplifter be seen doing all of the following:

(1) Taking the merchandise
(2) Concealing it without having paid for it
(3) Ditching the merchandise

If there is any break at all in the surveillance of the suspected shoplifter, the business will be taking a poorly calculated risk in attempting to make an arrest.

A retailer must develop clear and legally sound procedures for detaining suspected shoplifters and safeguarding evidence. Local police departments can usually offer advice on the proper procedures to follow.

Most states also have laws called *civil recovery* or *civil demand* statutes, which allow retailers to forgo the hassles of the legal system and simply ask shoplifters to make restitution, including some costs. While some retailers make such requests while the suspected shoplifter is still in the custody of security personnel, loss prevention experts generally recommend that civil recovery be handled after the suspect has been released. At such time, a letter from the victimized business, on its own or via an attorney or third-party company, can be sent to the shoplifter, demanding statutorily set compensation, including the value of the item(s) stolen and damages.

A.18.2.1.2.2.1 Because of the risk of check fraud, some retail businesses have a policy of not accepting checks as payment for goods. The check policy should be posted in a location readily seen by customers.

A.18.2.1.2.2.2(3) Third-party checks such as payroll or government checks can be easily stolen.

A.18.2.1.2.3 Elements of the policy should include requiring credit card transactions to be checked electronically; checking the signature on the sales receipt against the signature on the card; and checking the validation and expiration dates on the credit card.

A.18.2.1.3 When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors' or contractors' management about their preemployment screening and drug testing practices.

A.18.2.1.4.1 Performing regular reviews of security procedures keeps management informed that maintenance programs are up to date, security personnel are patrolling the premises as required, and reports are being filed. The findings of the review should be adequately addressed by management. Management needs to also review all security-related incidents [illegible] resolved.

Management will regularly review its security needs and provide personnel to respond to emergencies and assist customers and employees as required. If contract security is utilized, the security contractor is responsible for the selection, training, and supervision of personnel and for complying with all state and local laws, rules, and regulations.

A.18.2.1.4.3 Management should consider having some of their security personnel visible, in an effort to deter criminal activity. Security personnel should patrol the premises on a regular schedule, but not in a predetermined pattern. Patrol rounds should include exterior grounds, building perimeter, parking areas, stairwells, exit and delivery corridors, and storage, receiving, and trash disposal areas. The number of security personnel on patrol can vary by time of day, day of the week, and the season of the year, depending on local security problems, peak traffic periods, and special events.

A.18.2.4 Retail establishments, in particular establishments that operate late at night, will benefit from an examination of their workplaces to determine if workplace violence is a potential hazard for their employees.

In response to this problem, the Occupational Safety and Health Administration (OSHA) has developed workplace violence prevention guidelines for use in the late-night retail industry, especially for convenience stores, liquor stores, and gasoline stations. Other types of retail establishments providing services during evening and night hours also will find this information helpful. The guidelines are intended to help retail employers design, select, and implement violence prevention programs based on the specific risk factors they identify in their particular workplaces.

Employee security training should include workplace violence policies. This can be particularly true for employees working at night in retail establishments when higher-level managers are not routinely on duty.

The National Institute for Occupational Safety and Health (NIOSH) has identified a number of factors that can increase a worker's risk for workplace assault. Those pertaining to late-night retail establishment include the following:

(1) Contact with the public
(2) Exchange of money
(3) Delivery of passengers, goods, or services
(4) Working alone or in small numbers
(5) Working late-night or early-morning hours
(6) Working in high-crime areas

Employees in some retail establishments are exposed to multiple risk factors. The presence of a single risk factor does not necessarily indicate that the risk of violence is a problem in a workplace. The presence of multiple risk factors or a history of workplace violence, however, should alert an employer that the potential for workplace violence is increased.

Research indicates that the greatest risk of work-related homicide comes from violence inflicted by third parties, such as robbers and muggers. Robbery and other crimes were the motive in 80 percent of workplace homicides across all industries in 1996. A large proportion of the homicides occurring in the retail sector are associated with robberies and attempted robberies. On average, one in 100 gun robberies results in a homicide. For this reason, effective programs that reduce the number of robberies should result in a decrease in the number of homicides.

Sexual assault is another significant occupational risk in the retail industry. Indeed, the risk of sexual assault for women is equal to or greater than the risk of homicide for employees in general. Sexual assault is usually not robbery related but can occur more often in stores with a history of robbery. These assaults occur disproportionately at night in the great majority of cases and involve a female clerk alone in a store. The risk factors for robbery and sexual assault overlap (e.g., working alone, working late at night, high-crime areas), so actions to reduce robbery can also be effective for preventing sexual assaults.

Because the major risk of death or serious injury to retail employees is from robbery-related violence, an effective prevention program will include, but not be limited to, steps to reduce the risk of robbery. In general, a business can reduce the risk of robbery by doing the following:

(1) Increasing the effort the perpetrator must expend (target hardening, controlling access, and deterring offenders)
(2) Increasing the risks to the perpetrator (entry/exit screening, formal surveillance by employees and others)
(3) Reducing the rewards to the perpetrator (removing the target, identifying property, and removing inducements)

Other deterrents that can reduce the potential for robbery include security cameras, time-release safes, other 24-hour business at the location, no easy escape routes or hiding places, and closing the store during the late-night hours.

A.18.3.2 There should be good visibility and no potential hiding places for assailants near these areas. Robberies have occurred when employees were disposing of the trash at night. Procedures, such as using two employees, are to be considered to ensure employee safety.

A.18.4.1.1 Businesses with large amounts of cash on hand are at greater risk to robbery. Cash in cash registers should be kept at the lowest possible level by removing extra cash and depositing it in a time-delay cash drop safe for later deposit in the bank. The times and routes of bank deposits must be varied. Post a sign stating that only limited cash is available, that the cash is kept in a time-delay safe, and that employees do not have access to the safe.

A.18.4.1.2 Burglars often look first for easy ways to enter premises: through unlocked doors, unlatched windows, and unsecured skylights. While some burglars have the expertise to pick a lock, in most cases, entry is made using physical force by smashing doors, crow-barring doors or windows, and breaking window glass. Some burglars have resorted to breaking through building walls with sledgehammers. The risk of burglary is also influenced by the store's hours of operation. Those that operate 24 hours a day, 7 days a week are the least vulnerable to burglary.

Burglary is a crime of opportunity. Research into the crime indicates that burglars look for places that offer the best opportunity for success. In choosing targets, burglars look for locations that contain something worth stealing and then select those locations that look easy to break into. Burglars appear to be strongly influenced by the look and feel of the business they are planning to burglarize. Consequently, if the exterior of a business appears to reflect attention to security, the burglar will likely look for an easier opportunity. Good locks, ironwork, and lighting all contribute to making a building appear secure.

A.18.4.1.3 The right type and class of safe or vault must be chosen for the valuables to be protected. Safes are either fire-resistive or burglary-resistant and are available in various protection classes (or levels). The higher the value of the items to be protected, the higher the level of protection afforded by the safe should be. UL has listings for safes in various protection classifications. The number of people with access to the combination must be kept to a minimum. The combination number may not be stored in an easily accessible place, such as a desk blotter, and the safe or vault must never be put in "day mode," in which only one number is needed to complete the combination. The combination must be changed on a regular basis.

A.18.4.3 The interior and the front and rear entrances of the premises should be well lit. Adequate outside lighting of the parking area and approaches during nighttime hours of operation enhance employee and customer protection. Local ordinances and building codes can mandate lighting requirements.

Δ **A.18.4.4** Landscaping serves the primary purpose of aesthetics, but it can also create security problems. Shrubbery can provide concealment for criminals when it is allowed to become overgrown, and trees can serve as a means of scaling fences or accessing rooftops if they are planted too close to the fence line or buildings. There are several guides for trimming of shrubbery and trees. One example is shrubbery should be kept to a maximum of 3 ft (0.91 m) in height and trees trimmed so that the bottom branches are a minimum of 7 ft (2.13 m) above the ground. This will provide a clear zone of approximately 4 ft (1.21 m) between the top of the shrubbery and bottom branches of the trees for surveillance purposes.

Landscaping can also be used as a deterrent to intrusion. Examples are as follows:

(1) Shrubbery with briars or thorns
(2) Thick plantings that are difficult to penetrate

A.18.4.5 Clear visibility into the store can serve as a deterrent to robbery because it will enable passersby and police patrols to observe activities inside. It will also enable employees to observe suspicious activities outside the store.

A.18.5.3.2 Executing a burglary involves locating and collecting items of value. Factors that affect the time burglars will spend on the premises include the skill and confidence of the burglar(s), whether valuables are stored in a safe or vault, the quality of the protection, and the anticipated response by the police or designated personnel. An intrusion detection system can deter a burglar. An alarm system that sends a signal to a monitoring station, which then dispatches designated personnel, is preferred. An alarm system that sounds a local bell is better than no alarm at all — at the very least, it might scare off the burglar.

A.18.5.3.3 If utilized, a video surveillance system can cover all entrances, exits, entrance ramps, elevators, stairwells, walkways, and parking areas. Lighting levels might have to be increased for proper operation of the video surveillance system. Signs stating that the area is under surveillance can serve a deterrent function. Fake cameras must never be used — they give a false sense of security. Video surveillance is a tool that can be used to record historical data that can assist the police in solving crimes.

A.18.6 Because of the significant risks they pose, parking facilities are to be afforded spe

A.19.1.1 The dilemma that office building owners and managers face is how to keep the building secure while allowing entry to legitimate users and exit under emergency conditions. While authorized personnel should be allowed to come and go with relative ease, unauthorized individuals' access should be restricted.

A.19.1.1.2 Security for buildings listed in 19.1.1.1 should be designed according to the requirements of the U.S. Department of Justice (DOJ) publication, *Vulnerability Assessment of Federal Facilities*.

A.19.1.2.1 An effective security program will depend on coordinated development and implementation of the security plan between management, security personnel, and employees. Often, the difference between the success and failure of a security program is realized through management's degree of commitment to and support for the program.

Ideally, security for an office building should be considered during the architectural planning stages. It is then that crime prevention measures, including access control systems, can be most economically implemented. Unfortunately, security considerations are often after the fact, occurring only after the building has been designed.

An effective security plan cannot stop all crime. Sales personnel should be advised not to make oral promises regarding the security of the facility. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.19.1.3.2(6) Research should be conducted to determine the state of the neighborhood surrounding the facility. The research should focus on whether the neighborhood has remained stable or has deteriorated. A history of violent and property crime in the immediate neighborhood and on the premises should be compiled and reviewed.

A relationship with local law enforcement agencies should be developed to make them familiar with the property. The local police should be requested to include the facility in patrol routes. An open line of communication should be maintained with the local police and federal authorities to obtain information on crime and crime trends in the neighborhood or area.

Management should be active in local security associations or industry trade groups as a means of sharing common security concerns and solutions. Management should consider joining emergency response organizations, including the Department of Homeland Security Information Sharing Network (DHS INFO), which sends members real-time threat information via e-mail, pagers, and cell phones.

A.19.2 Contact information should be posted where it can always be seen. If the reception desk is constantly attended, the information may be posted there, but otherwise contact information should be visible from the exterior of the building.

A.19.2.1.1.2 In unoccupied offices, purses should not be left on top of desks or on the floor, and wallets and checkbooks should not be left in jackets.

A.19.2.1.1.3 Security awareness should be provided. Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth.

A.19.2.1.1.4 One way to provide notification is by monthly

A.19.2.1.2.1 The person requested by the visitor should confirm the appointment. If policy requires it, visitors should be escorted to their destination.

A.19.2.1.2.2.2 It should be noted that if employees are not required to wear badges, visitors have only to remove theirs to look like employees.

A.19.2.1.3 Contractors, maintenance, housekeeping, and other vendors should display identification badges acceptable to facility management. Custodial personnel reporting to the building after the end of the normal business day, whether employees or a contract service, should be required to check in and check out with security personnel. Maintenance, housekeeping, and other service personnel who operate on all floors or areas of the building should be issued distinctive uniforms and identification badges. The supply of uniforms and badges should be controlled.

A.19.2.2 A messenger center for packages, lunches, and other deliveries should be established. Messengers should not be allowed to roam the building freely.

A.19.3.1.2 A door of solid construction should be used to secure loading openings. A video surveillance camera can be installed for continuous surveillance of the door and ramp. An intercom should be available at the entrance to identify persons or vehicles without machine readable credentials. The freight elevator doors leading into the shipping and receiving area should be secured during periods of nonuse.

A.19.3.1.3 Different business settings or structures, such as high-rise office buildings or campus-style settings of multiple buildings, require different access control approaches.

In an office building occupied by one company, ground- or street-level access control, combined with additional controls at sensitive areas, can be set up.

In multitenant buildings, security is more complex. Access control in the main lobby will usually serve as a first line of defense. For tenants that occupy one entire floor above the lobby level, the elevator lobby on the floor can serve as a second control point. If there are several tenants on a floor, the tenants should provide some type of control at their entrance door. For tenants that occupy several floors served by one elevator bank, access control can be set up at the street-level lobby to their elevator bank. If there is no dedicated elevator bank, programming elevators to stop at only one floor, especially during nonbusiness hours, coupled with the use of internal stairs, allows for economical single-point control.

In a campus-style environment with several buildings, multiple visitor reception points can be needed. A lobby with a receptionist controlling access to the interior is typical. An economical alternative is a telephone in a secured lobby.

The level of security needed will depend on the degree of risk involved. Businesses with valuable products, trade secrets, confidential or sensitive company information, expensive equipment and furnishings, or valuable art collections are at greater risk to unauthorized intruders and therefore require a higher level of access control.

The types of tenants and their respective business activities also affect the level of security needed. An example is an office building with a restaurant or theater tenant. This type of tenant is usually open after normal business hours and on weekends, requiring additional security

building with residential tenants, who require 24-hour access, is another example of unique security needs.

A.19.3.2.1 Entrance areas provide the first impression of the level of security awareness in a building. An office building should not give the appearance of being open to casual visitors. Visitors should be funneled to the reception desk and not be able to access secure areas without proper authorization.

If a reception or security desk is provided in the lobby of the building, it should be positioned to provide for the best view of doorways and persons entering the building. A receptionist or guard should be stationed at the desk when the building is open.

If there is an automated access control system for employees, the entrance should be located as close as is practical to the reception desk. If there is no automated access control system, a guard or receptionist should check employee identification.

A.19.3.2.2 Perimeter entrances should be secured during nonbusiness hours. Entry point(s) should be designated for after-hours access. A program exists to ensure that entrances that are not needed for entry or exit are secured.

A.19.3.2.3 Emergency exits should be alarmed and monitored to detect unauthorized use.

A.19.5.2 Some examples of this type of protection for elevator cars are convex or plain mirrors or video surveillance.

A.19.5.3.4 Twenty-four-hour video surveillance and recording are desirable as a deterrent. Requirements depend on the results of an assessment of the security threat. Time-lapse video recordings are also highly valuable as a source of evidence and investigative leads. Warning signs advising of 24-hour surveillance act as a deterrent in protecting employees and facilities. While the video surveillance system can be monitored at the reception desk, it is usually preferable that it be monitored at a separate security console.

A.20.1.2.2.1 A facility safety plan and a security plan often address the same or similar concerns. Many of the steps to limit physical damage should already be part of the process safety management system. These steps can be related either to the design of the facility and its processes or to procedures implemented.

An evaluation of current safety and security systems should be included in the SVA. Factors that should be reviewed for applicability and consideration include the following:

(1) The location of the site in relation to other structures, facilities, and population centers
(2) The accessibility of the site
(3) The building age, construction type, and openings
(4) Hours of operation
(5) Hazardous materials or processes at the site

Sites that are close to other structures or facilities may be vulnerable from shared perimeters, buildings that are close together, or hazardous processes. Some hazardous materials or processes can be particularly attractive targets because of the potential for greater consequences.

Older buildings might be more vulnerable because they have more windows, while some newer buildings are designed for easy access. A facility that operates 24 hours a day might need less security, because there are always people on-site, than a

The existing security systems (e.g., fences, security lighting, security patrols, or electronic premises security systems) should be evaluated to establish if they are adequate to limit access to the site.

A.20.1.2.2.2 Decisions about improving site security should be made after an evaluation of how vulnerable the site is to threats and what additional measures, if any, are appropriate to reduce this vulnerability. Decisions about security should be made based on the circumstances at the particular facility.

A.20.2.1.1 Maintaining good labor relations will help to protect the facility from actions by employees or contractors. Important labor relations considerations are as follows:

(1) Open negotiations
(2) Workplace policies emphasizing that violence and substance abuse are not tolerated
(3) Adequate training and resources

The goal of good labor relations should be to develop the capacity of the workforce and management to identify and solve problems by working together.

A.20.2.1.1.2 Security awareness training should be provided. Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth.

A.20.2.1.1.3 Emergency shutdown procedures should be included as part of the written operating procedures. Emergency procedures are particularly important if there are processes that operate under extreme conditions (high or low pressures or temperatures). Rapid shutdown can create further hazards if done improperly.

A.20.2.1.2.4 It should be noted that if employees are not required to wear badges, visitors have only to remove theirs to look like employees.

A.20.2.2.2 The inventory of hazardous materials should be limited to the minimum needed for operation. This practice limits the quantity of a hazardous material that could be released. Another practice to consider is substituting less hazardous substances when possible to make processes inherently safer.

As a matter of good practice as well as site security, storage tanks and delivery vehicles not in use should be disconnected from piping, transfer hoses, or distribution systems, which are often vulnerable to an adversarial event.

A.20.3.2 IES G 1, *Guideline for Security Lighting for People, Property, and Public Spaces,* is for design and implementation of security lighting. The guideline is intended for use by property owners and managers, crime prevention specialists, law enforcement and security professionals, risk managers, lighting specifiers, contractors, the legal profession, and homeowners concerned about security and the prevention of crime. It covers basic security principles, illumination requirements for various types of properties, protocol for evaluating current lighting levels for different security applications, and security survey and crime search methodology. Guidelines include exterior and interior security lighting practices for the reasonable protection of persons and property. There are many complexities to exterior lighting design, including but not limited to "dark sky" compliance, light wash through adjacent properties, and energy conservation. Proper illumination should encourage authorized users to occupy spaces and discourage intruders.

Annex B Homeland Security Advisory System

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

B.1 General. A recommended threat response elevation system was originally developed by the United States Department of Homeland Security (DHS). As threat conditions rise, it is recommended that facilities implement an appropriate corresponding set of protective measures to further reduce vulnerability and increase response capability.

The following threat response recommendations are voluntary.

B.2 Threat Conditions and Associated Protective Measures. There is always a threat of a terrorist attack. Each threat condition assigns a recommended level of alert appropriate to the increasing risk of terrorist attacks. Threat conditions contain suggested protective measures that the government and the public can take, recognizing that the heads of federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures.

B.2.1 Normal Condition. A normal condition is when there is a low risk of terrorist attacks. The private sector should consider the following protective measures:

(1) Refine and exercise prearranged protective measures.
(2) Ensure that personnel receive proper training on the Homeland Security Advisory System and specific prearranged department or agency protective measures.
(3) Institute a process to ensure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities. Homeowners and the general public can develop a household disaster plan and assemble a disaster supply kit.
(4) Check communications with designated emergency response or command locations.
(5) Review and update emergency response procedures.
(6) Provide the public with any information that would strengthen its ability to act appropriately.

Homeowners and the general public, in addition to the actions taken for the low threat condition, should take the following steps:

(1) Update their disaster supply kits.
(2) Review their household disaster plans.
(3) Hold household meetings to discuss what members would do and how they would communicate in the event of an incident.
(4) Develop more detailed household communications plans.
(5) If they are apartment residents, discuss with building managers steps to be taken during an emergency.
(6) If they have special needs, discuss their emergency plans with friends, family, or employers.
(7) Increase surveillance of critical locations.
(8) Coordinate emergency plans with nearby jurisdictions as appropriate.

(9) Assess whether the precise characteristics of the threat require the further refinement of prearranged protective measures.
(10) Implement, as appropriate, contingency and emergency response plans.

Homeowners and the general public, in addition to the actions taken for the normal threat conditions, should take the following steps:

(1) Be observant of any suspicious activity and report it to authorities
(2) Contact neighbors to discuss their plans and needs
(3) Check with school officials to determine their plans for an emergency and procedures to reunite children with parents and caregivers
(4) Update household communications plans

B.2.2 Elevated Condition. An elevated condition is declared when there is a credible threat risk. In addition to the measures taken in the previous threat conditions, the private sector should consider the following protective measures:

(1) Coordinate necessary security efforts with federal, state, and local law enforcement agencies, the National Guard, or other security and armed forces.
(2) Take additional precautions at public events, possibly considering alternative venues or even cancellation.
(3) Prepare to execute contingency procedures, such as moving to an alternative site or dispersing the workforce.
(4) Restrict access to a threatened facility to essential personnel only.

Homeowners and the general public, in addition to the actions taken for the normal threat conditions, should take the following steps:

(1) Review preparedness measures (including evacuation and sheltering) for potential terrorist actions, including chemical, biological, and radiological attacks.
(2) Avoid high-profile or symbolic locations.
(3) Exercise caution when traveling.

B.2.3 Imminent Condition. An imminent condition reflects a credible, specific, and imminent threat risk. Under most circumstances, the protective measures for an imminent condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in normal and elevated threat conditions, the private sector should consider the following general measures:

(1) Increase or redirect personnel to address critical emergency needs.
(2) Assign emergency response personnel and pre-position and mobilize specially trained teams or resources.
(3) Monitor, redirect, or constrain transportation systems.
(4) Close public and government facilities not critical for continuity of essential operations, especially public safety.

Homeowners and the general public, in addition to the actions taken for the previous threat conditions, should take the following steps:

(1) Avoid public gathering places such as sports arenas, holiday gatherings, or other high-risk locations.
(2) Follow official instructions about restrictions to normal activities.
(3) Contact employers to determine status of work.
(4) Listen to the radio and TV for possible advisories or warnings.
(5) Prepare to take protective actions such as sheltering-in-place or evacuation if instructed to do so by public officials.

B.3 Preparing for Terrorism. Wherever they are, individuals should be aware of their surroundings. The very nature of terrorism suggests there might be little or no warning.

B.3.1 Individuals should take the following steps:

(1) Take precautions when traveling.
(2) Be aware of conspicuous or unusual behavior.
(3) Do not accept packages from strangers.
(4) Do not leave luggage unattended.
(5) Promptly report to police or security personnel unusual behavior, suspicious packages, and strange devices.
(6) Do not be afraid to move or leave if you feel uncomfortable or if something does not seem right.
(7) Learn where emergency exits are located in buildings you frequent. Notice where exits are when you enter unfamiliar buildings. Plan how to get out of a building, subway, or congested public area or traffic. Note where staircases are located. Notice heavy or breakable objects that could move, fall, or break in an explosion.
(8) Assemble a disaster supply kit at home and learn first aid. Separate the supplies to take if evacuation is necessary, and put them in a backpack or container, ready to go.
(9) Be familiar with different types of fire extinguishers and how to locate and use them. Know the location and availability of hard hats in buildings in which you spend a lot of time.

B.3.2 Private sector facilities should take the following steps:

(1) Consider all the precautions prescribed for individuals.
(2) Develop written policies and procedures for terrorist events, train all personnel to them, and test their effectiveness.
(3) Provide a prepared on-site area of refuge for guests and employees should an off-site consequence prevent travel from the facility. Preparations should include provision of nonperishable food and drinking water, battery-powered commercial radio or television, first aid supplies, sanitation supplies, flashlights, and so forth.

B.4 Protection Against Cyberattacks. Cyberattacks target computer or telecommunication networks of critical infrastructures such as power systems, traffic control systems, or financial systems. Cyberattacks target information technologies (IT) in three different ways. The first type of attack is a direct attack against an information system through the wires alone (hacking). The second type of attack takes the form of a physical assault against a critical IT element. The third type of attack originates from the inside as a result of a trusted party with access to the system compromising information.

Both individuals and private sector facilities should be prepared for the following situations:

(1) To be without services that people normally depend on and that could be disrupted — electricity, telephone service, natural gas, gasoline pumps, cash registers, ATM machines, and Internet transactions
(2) To respond to official instructions (such as general evacuation, evacuation to shelter, or shelter-in-place) if a cyberattack triggers other hazards, for example, hazardous materials releases, nuclear power plant incident, dam or flood control system failures

B.5 Preparing for a Building Explosion. Explosions can collapse buildings and cause fires. Both individuals and private sector facilities can do the following:

(1) Regularly review and practice emergency evacuation procedures.
(2) Know where emergency exits are located.
(3) Keep fire extinguishers in proper working order. Know where they are located and learn how to use them.
(4) Learn first aid.

Additionally, private sector facilities should keep the following items in a designated place on each floor of the building:

(1) Portable, battery-operated radio and extra batteries
(2) Several flashlights and extra batteries
(3) First aid kit and manual
(4) Several hard hats
(5) Fluorescent tape to rope off dangerous areas

B.6 Bomb Threats. If a bomb threat is received, get as much information from the caller as possible. Keep the caller on the line and record everything that is said. Then notify the police and facility security.

Following notification of a bomb threat, do not touch or handle any suspicious packages. Clear the area around suspicious packages and notify the police immediately. In evacuating a building, avoid windows, glass doors, and other potentially hazardous areas. Building evacuation procedures should keep sidewalks and streets to be used by emergency officials or others still exiting the building clear and unobstructed.

B.6.1 Suspicious Parcels and Letters. Be wary of suspicious packages and letters. They can contain explosives or chemical or biological agents. Be particularly cautious at high-profile facilities.

Over the years, postal inspectors have identified certain characteristics that ought to trigger suspicion about a parcel, including the following:

(1) An unexpected delivery or from someone unfamiliar
(2) No return address or one that cannot be verified as legitimate
(3) Marked with restrictive endorsements, such as "Personal," "Confidential," or "Do Not X-Ray"
(4) Protruding wires or aluminum foil, strange odors, or stains
(5) City or state in the postmark that does not match the return address
(6) Unusual weight given its size, lopsidedness, or odd shape
(7) Marked with threatening language
(8) Inappropriate or unusual labeling
(9) Excessive postage or excessive packaging material such as masking tape and string
(10) Misspellings of common words
(11) Addressed to someone no longer with the organization or otherwise outdated
(12) Incorrect titles or title without a name
(13) Not addressed to a specific person
(14) Handwritten or poorly typed addresses

With suspicious envelopes and packages other than those that might contain explosives, take the following additional steps against possible biological and chemical agents:

(1) Refrain from eating or drinking in a designated mail-handling area.
(2) Place suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents. Never sniff or smell suspect mail.
(3) If you do not have a container, then cover the envelope or package with anything available (e.g., clothing, paper, trash can) and do not remove the cover.
(4) Leave the room and close the door or section off the area to prevent others from entering.
(5) Wash your hands with soap and water to prevent spreading any hazardous substance to your face.
(6) If you are at work, report the incident to facility security officials, who should notify police and other authorities without delay.
(7) List all people who were in the room or area when the suspicious letter or package was recognized. Give a copy of this list to both local public health authorities and law enforcement officials for follow-up investigations and advice.
(8) If you are at home, report the incident to local police without delay.

B.6.2 Explosion. In the event of an explosion, the following actions should be taken:

(1) Evacuate the building as quickly as possible.
(2) Instruct personnel to do the following:
    (a) Do not stop to retrieve personal possessions or make phone calls.
    (b) Get under a sturdy table or desk if debris and other objects are falling.
    (c) Leave quickly after debris has stopped falling; watch for weakened floors, stairs, and additional falling debris as you exit.

B.6.3 Fire. In the event of a fire, the following actions should be taken:

(1) Stay low to the floor and exit the building as quickly as possible.
(2) Cover nose and mouth with a wet cloth.
(3) When approaching a closed door, use the back of the hand to feel the lower, middle, and upper parts of the door. Never use the palm or fingers to test for heat: burning those areas could impair your ability to escape a fire (i.e., using a ladder and crawling).
(4) If the door is NOT hot, open it slowly and make sure that fire or smoke is not blocking the escape route. If the escape route is blocked, shut the door immediately and use an alternative escape route, such as a window. If the escape route is clear, leave immediately through the door. Be prepared to crawl — smoke and heat rise, causing the air near the floor to be cleaner and cooler.
(5) If the door is hot, do NOT open it. Escape through a window. If you cannot escape, hang a white or light-colored sheet outside the window, alerting fire fighters to your presence.
(6) Thick smoke and poisonous gases collect first along the ceiling. Stay below the smoke at all times.

B.6.4 Trapped in Debris. In the event you are trapped by debris, the following actions should be taken:

(1) Do not light a match or lighter.
(2) Do not move about or kick up dust. Cover your mouth with a handkerchief or clothing.
(3) Rhythmically tap on a pipe or wall so that rescuers can [illegible] a whistle if one is available.

Shout only as a last resort when you hear sounds and think someone will hear you — shouting can cause inhalation of dangerous amounts of dust.

B.7 Chemical and Biological Weapons. In the event of a chemical or biological weapon attack, authorities will provide instructions on the best course of action. This can be to evacuate the area immediately, to seek shelter at a designated location, or to take immediate shelter where you are and seal the premises. The best way to protect yourself is to take emergency preparedness measures ahead of time and to get medical attention, if needed, as soon as possible.

B.7.1 Chemical Weapons. Chemical warfare agents are poisonous vapors, aerosols, liquids, or solids that have toxic effects on people, animals, or plants. They can be released by bombs; sprayed from aircraft, boats, or vehicles; or used as a liquid to create a hazard to people and the environment. Some chemical agents are odorless and tasteless. They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (several hours to several days). While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly. Chemical agents are also difficult to produce.

The six types of agents are as follows:

(1) Lung-damaging (pulmonary) agents such as phosgene
(2) Cyanide
(3) Vesicants or blister agents such as mustard
(4) Nerve agents such as GA (tabun), GB (sarin), GD (soman), GF (cyclosarin), and VX
(5) Incapacitating agents such as BZ
(6) Riot-control agents (similar to Mace)

B.7.2 Biological Weapons. Biological agents are organisms or toxins that can kill or incapacitate people, livestock, and crops. The three basic groups of biological agents that would be likely to be used as weapons are bacteria, viruses, and toxins.

Bacteria are small free-living organisms that reproduce by simple division and are easy to grow. The diseases they produce often respond to treatment with antibiotics.

Viruses are organisms requiring living cells in which to reproduce and are intimately dependent on the body they infect. Viruses produce diseases that generally do not respond to antibiotics. However, antiviral drugs are sometimes effective.

Toxins are poisonous substances typically found in, and extracted from, living plants, animals, or microorganisms; some toxins, however, can be produced or altered by chemical means. Select toxins can be treated with specific antitoxins and selected drugs.

Most biological agents are difficult to grow and maintain. Many break down quickly when exposed to sunlight and other environmental factors, while others, such as anthrax spores, are very long-lived. They can be dispersed by spraying them in the air, by infecting animals that carry the disease to humans, or through food and water contamination, as follows:

(1) Aerosols — Biological agents are dispersed into the air, forming a fine mist that can drift for miles. Inhaling the agent can cause disease in people or animals.
(2) Animals — Some diseases are spread by insects and animals such as fleas, mice, flies, and mosquitoes. Deliberately spreading diseases through livestock is also referred to as agroterrorism.
(3) Food and water contamination — Some pathogenic organisms and toxins can persist in food and water supplies. Cooking food and boiling water will kill most microbes and deactivate most toxins.
(4) Person-to-person — Person-to-person spread of infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and the Lassa viruses.

B.7.3 What to Do to Prepare for a Chemical or Biological Attack. A disaster supply kit should be assembled to include the following:

(1) Battery-powered commercial radio with extra batteries.
(2) Nonperishable food and drinking water.
(3) Roll of duct tape and scissors.
(4) Plastic for doors, windows, and vents for the room in which you will take shelter — this should be an internal room where air that can contain hazardous chemical or biological agents can be blocked out. To save critical time during an emergency, sheeting should be premeasured and cut for each opening.
(5) First aid kit.
(6) Sanitation supplies, including soap, water, and bleach.

B.7.4 What to Do During a Chemical or Biological Attack. The following safeguards should be observed:

(1) Listen to the radio for instructions from authorities, such as whether to remain inside or to evacuate.
(2) If you are instructed to remain in your home, the building where you are, or other shelter during a chemical or biological attack, do the following:
    (a) Turn off all ventilation, including furnaces, air conditioners, vents, and fans.
    (b) Seek shelter in an internal room, preferably one without windows.
    (c) Seal the room with duct tape and plastic sheeting. Ten square feet of floor space per person will provide sufficient air to prevent carbon dioxide buildup for up to 5 hours.
(3) Remain in protected areas where toxic vapors are reduced or eliminated; be sure to have a battery-operated radio at hand.
(4) If you are caught in an unprotected area, do the following:
    (a) Attempt to get upwind of the contaminated area.
    (b) Attempt to find shelter as quickly as possible.
    (c) Listen to your radio for official instructions.

B.7.5 What to Do After a Chemical Attack. Immediate symptoms of exposure to chemical agents can include blurred vision, eye irritation, difficulty breathing, and nausea. A person affected by a chemical or biological agent requires immediate attention by professional medical personnel. If medical help is not immediately available, decontaminate yourself and assist in decontaminating others. Decontamination is needed within minutes of exposure to minimize health consequences. (However, you should not leave the safety of a shelter to go outdoors to help others until authorities announce it is safe to do so.) The following steps should be taken:

(1) Use extreme caution when helping others who have been exposed to chemical agents.
(2) Remove all clothing and other items in contact with the body. Contaminated clothing normally removed over the head should be cut off to avoid contact with the eyes, ...ning into a plastic bag if

possible. Decontaminate hands using soap and water. Remove eyeglasses or contact lenses. Put glasses in a pan of household bleach to decontaminate.
(3) Remove all items in contact with the body.
(4) Flush eyes with lots of water.
(5) Gently wash face and hair with soap and water; then thoroughly rinse with water.
(6) Decontaminate other body areas likely to have been contaminated. Blot (do not swab or scrape) with a cloth soaked in soapy water and rinse with clear water.
(7) Change into uncontaminated clothes. Clothing stored in drawers or closets is likely to be uncontaminated.
(8) If possible, proceed to a medical facility for screening.

B.7.6 What to Do After a Biological Attack. In many biological attacks, people will not know they have been exposed to an agent. In such situations, the first evidence of an attack can be when you notice symptoms of the disease caused by exposure to an agent — seek immediate medical attention for treatment.

In some situations, like the anthrax letters sent in 2001, people can be alerted to a potential exposure. Pay close attention to all official warnings and instructions on how to proceed. The delivery of medical services for a biological event might be handled differently to respond to increased demand. Again, it will be important to pay attention to official instructions via radio, television, and emergency alert systems.

If your skin or clothing comes in contact with a visible, potentially infectious substance, remove and bag the clothes and personal items and wash yourself with warm soapy water immediately. Put on clean clothes and seek medical assistance.

For more information, visit the web site for the Centers for Disease Control and Prevention, www.cdc.gov.

B.8 Nuclear and Radiological Attack. Nuclear explosions can cause deadly effects — blinding light, intense heat (thermal radiation), initial nuclear radiation, blast, fires started by the heat pulse, and secondary fires caused by the destruction. They also produce radioactive particles, called *fallout*, that can be carried by wind for hundreds of miles.

Terrorist use of a radiological dispersion device (RDD) — often called a "dirty nuke" or "dirty bomb" — is considered far more likely than use of a nuclear device. These radiological weapons are a combination of conventional explosives and radioactive material designed to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Such radiological weapons appeal to terrorists because they require very little technical knowledge to build and deploy compared to that for a nuclear device. Also, these radioactive materials are used widely in medicine, agriculture, industry, and research and thus are much more readily available and easier to obtain than weapons-grade uranium or plutonium.

Terrorist use of a nuclear device would probably be limited to a single smaller "suitcase" weapon. The strength of such a weapon would be in the range of the bombs used during World War II. The nature of the effects would be the same as a weapon delivered by an intercontinental missile, but the area and severity of the effects would be significantly more limited.

There is no way of knowing how much warning time there would be before an attack by a terrorist using a nuclear or radiological weapon. A surprise attack remains a possibility.

The danger of a massive strategic nuclear attack on the United States involving many weapons receded with the end of the Cold War. However, some terrorists have been supported by nations that have nuclear weapons programs.

If there were threat of an attack from a hostile nation, people living near potential targets could be advised to evacuate, or they could decide on their own to evacuate to an area not considered a likely target. Protection from radioactive fallout would require taking shelter in an underground area or in the middle of a large building.

In general, potential targets include the following:

(1) Strategic missile sites and military bases
(2) Centers of government, such as Washington, DC, and state capitals
(3) Important transportation and communication centers
(4) Manufacturing, industrial, technology, and financial centers
(5) Petroleum refineries, electrical power plants, and chemical plants
(6) Major ports and airfields

Taking shelter during a nuclear attack is absolutely necessary. There are two kinds of shelters — blast and fallout. Blast shelters offer some protection against blast pressure, initial radiation, heat, and fire, but even a blast shelter could not withstand a direct hit from a nuclear detonation. Fallout shelters do not need to be specially constructed for that purpose. They can be any protected space, provided that the walls and roof are thick and dense enough to absorb the radiation given off by fallout particles. The three protective factors of a fallout shelter are as follows:

(1) *Shielding.* The more heavy, dense materials — thick walls, concrete, bricks, books, and earth — between you and the fallout particles, the better.
(2) *Distance.* The more distance between you and the fallout particles, the better. An underground area, such as a home or office building basement, offers more protection than the first floor of a building. A floor near the middle of a high-rise can be better, depending on what is nearby at that level on which significant fallout particles would collect. Flat roofs collect fallout particles so the top floor is not a good choice, nor is a floor adjacent to a neighboring flat roof.
(3) *Time.* Fallout radiation loses its intensity fairly rapidly. In time, you will be able to leave the fallout shelter. Radioactive fallout poses the greatest threat to people during the first 2 weeks, by the end of which time it will have declined to about 1 percent of its initial radiation level.

It is important to remember that any protection, however temporary, is better than none at all, and the more shielding, distance, and time that can be taken advantage of, the better.

B.8.1 Electromagnetic Pulse. In addition to other effects, a nuclear weapon detonated in or above the earth's atmosphere can create an electromagnetic pulse (EMP), which is a high-density electrical field. An EMP acts like a bolt of lightning but is stronger, faster, and briefer. An EMP can seriously damage electronic devices connected to power sources or antennas, such as communications systems, computers, electrical appliances, and automobile or aircraft ignition systems. The damage could range from a minor interruption to actual burnout of components. Most electronic equipment within 1000 miles ear detonation could be affec-