PRINCIPLES OF DESIGN FOR RISK REDUCTION RELATED TO OPERATIONAL SECURITY MEASURES 5

Operational security measures for commercial buildings augment the blast and CBR physical protective measures by establishing the capability to deter, detect, delay, and respond to these threats, as well as other harmful acts. Operational security measures encompass the physical security systems, the security policies and procedures, and the personnel resources committed to protecting commercial buildings. This chapter reviews the range of operational security measures available to commercial facilities to counter blast and CBR threats and addresses considerations for applying these measures to retail, office, and multifamily residential facilities, and hotels. The chapter concludes with an examination of the integration of operational and physical protective measures, including the relative flexibility of operational measures and the resulting tradeoffs during implementation.

5.1 OVERVIEW OF OPERATIONAL SECURITY MEASURES

Operational security measures work in conjunction with blast and CBR measures to protect personnel, equipment, and intellectual property. A baseline of protective measures established at commercial facilities might include locking doors, lighting parking lots, and controlling access to small expensive items. Beyond this baseline, additional security measures are commonly added to counter specific threats. These measures might include procedures as simple as checking the picture and date on an identification card. Additional security measures can also include sophisticated systems, such as biometric identification, metal detectors, video assessment and surveillance systems, armed security personnel, and even chemical and radiation detectors.

OPERATIONAL SECURITY MEASURES

- Detection and Assessment Measures
- Interdiction and Response Measures
- Procedural Measures
- Preparedness Measures
- Security Master Planning

Operational security measures can be divided into five basic components: detection and assessment measures, interdiction and response measures, procedural measures, preparedness measures, and security master planning.

5.2 DETECTION AND ASSESSMENT MEASURES

Detection and assessment measures for blast events and CBR threats include exterior intrusion detection, interior intrusion detection, CCTV systems, access control systems, vehicle inspections, duress alarms, and mail/package screening.

5.2.1 EXTERIOR INTRUSION DETECTION SYSTEMS

Exterior intrusion detection systems are used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones along fences or around buildings or for detecting unauthorized access to critical outdoor infrastructure (transformers, water tanks, etc.). Generally these systems use infrared, (see Figure 5-1) seismic, microwave, or video motion technologies to alert security personnel to an encroachment. Because of the nature of the outdoor environment, exterior sensors are more susceptible to nuisance and environmental alarms than interior sensors. The use of dual technology sensors and a proper assessment method is key to an effective system.

Figure 5-1: Doorway with balanced magnetic switch and passive infrared motion sensor.
SOURCE: TERRENCE RYAN

5.2.2 INTERIOR INTRUSION DETECTION SYSTEMS

Interior intrusion detection measures, like exterior systems, are designed to detect penetration or attempted penetration through perimeter barriers. Interior sensors can be deployed at a facility's perimeter or in an interior space. An interior asset is one contained within a cube with sensors protecting all six faces, such as walls, ceilings, and floors, to include duct openings, doors, and windows. Tamper protection and access/secure mode capabilities should be considered when planning interior systems. Interior sensors include:

- Structural vibration sensors
- Glass-breakage sensors
- Passive ultrasonic sensors
- Balanced magnetic switches
- Grid wire sensors
- Microwave motion sensors
- Passive infrared motion sensors
- Dual technology sensors
- Video motion sensors

DUAL TECHNOLOGY SENSORS

Dual technology sensors use two technologies in a logical combination to reduce false alarms. One example is a combination of a microwave sensor and a passive infrared sensor that must activate simultaneously to create an alarm.

5.2.3 VIDEO ASSESSMENT AND SURVEILLANCE SYSTEMS

Video assessment and surveillance systems may be used to conduct access control, surveillance, and video motion detection. Access control applications include monitoring building entrances, loading docks, and other access points. Surveillance applications include maintaining observation over large or concentrated areas, such as site access points, parking lots, building perimeters, key interior areas, or points of alarm. Video motion detection applications have sensors that generate an alarm when an intruder enters a selected portion of a camera's field of view. They can be programmed to activate alarms, initiate recording, or prompt other designated actions when motion is detected by a security camera.

- **Interior Applications.** Alarm assessment, card reader event assessment, emergency exit activation assessment, and surveillance of lobbies, corridors, and open areas.

- **Exterior Applications.** Alarm assessment, individual zones and portal assessment, specific paths and areas, exclusion areas, and surveillance of activities.

- **Video Motion Detection.** Video motion sensors are available on most digital video recorders (DVRs) used in security applications. The sensor processes and compares successive images against predefined alarm criteria. The system usually provides adjustable windows that can be positioned to monitor selected points of the video image. Some DVRs can be programmed to monitor very specific fields of view for specific types of motion in order to increase system effectiveness and minimize extraneous detections.

Video assessment and surveillance systems may be monitored in real time or recorded for later viewing (see Figure 5-2). Systems designed for one usage may not be optimized for the other.

ADDITIONAL VIDEO ASSESSMENT AND SURVEILLANCE SYSTEMS CONSIDERATIONS

- Plan camera placement to provide adequate coverage of vehicle and pedestrian movements along perimeter fence lines, site, roadway and parking lot access points, building exteriors, entrances, emergency exits, and utility systems.

- Use the integration features of modern Pan Tilt Zoom cameras systems to point and focus on cues from door contacts and switches, interior motion detection devices, or other sensors.

- Integrate landscaping efforts with camera placement initiatives. Control plantings and tree and shrubbery growth to avoid obstructing camera fields of view.

- Perform a lighting survey to ensure lighting levels are adequate and consistent with camera equipment manufacturer specifications.

- Train staff members on the use (and limitations) of the camera system.

- Video motion sensors can greatly improve the efficiency of security personnel monitoring security cameras by alerting them when motion is detected.

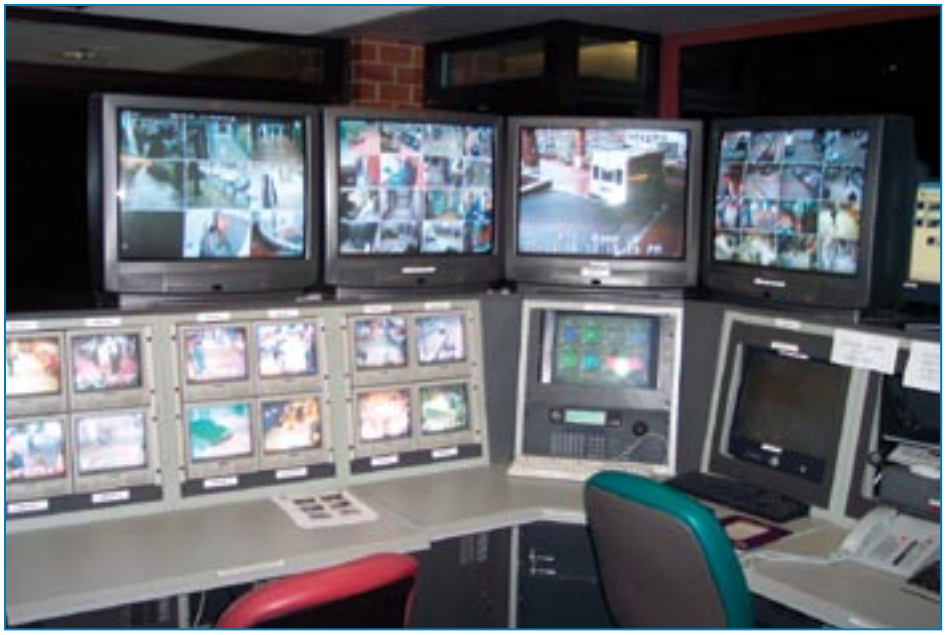

Figure 5-2: Video assessment and surveillance systems.
SOURCE: BOB CIZMADIA

5.2.4 ACCESS CONTROL SYSTEMS

The building layout, rate and flow of employees and visitors, threat level, personnel available, and types of technical equipment installed are considerations for establishing access control measures. A screening plan should be comprehensive to permit authorized personnel to conduct their business with minimum delay, but provide access to only those with a legitimate need. Access control measures normally consist of a public access control area, a walk-through metal detector and/or hand-held metal detector, and an entry control system.

- **Public Access Control Area.** This allows for identifying and screening of visitors before admitting them into restricted areas (see Figure 5-3).

- **Walk-Through Metal Detector and/or Hand-Held Metal Detector.** Metal detectors are intended to detect the presence of concealed firearms or other weapons while avoiding the intrusiveness of individual searches or frisking. Additionally, screening may detect the presence of concealed electronic devices (such as hidden transmitters) and explosive devices having metal components.

- **Entry Control Systems.** The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals. Entry control can be enforced physically with

Figure 5-3: Blast effects related to access control. SOURCE: MICHAEL KAMINSKAS

guards or automatically using entry control devices. For a guard system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry. For an automated system, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage. All entry control systems control passage using one or more of three basic techniques: a Personal Identification Number, a credential, or an identifying feature like a fingerprint. Automated entry control devices based on these techniques are grouped into three categories: code, credential, and biometric devices.

5.2.5 VEHICLE INSPECTION SYSTEMS

Vehicle inspection systems employ personnel to examine entering vehicles in accordance with predetermined guidelines (see Figure 5-4).

Figure 5-4: Entry control point.
SOURCE: TERRENCE RYAN

Inspections may be appropriate at low and high threat locations. At low threat locations, guards may only inspect a vehicle driver's identification or a facility parking sticker. At higher threat locations, guards may inspect the vehicle and occupants' identification, vehicle interior, undercarriage, engine compartment, interior, trunk, and gas-fill cover area. Inspections should occur as far from critical site facilities as possible (preferably at the site perimeter). The inspection area may include vehicle arresting devices that prevent vehicles from tailgating or from leaving the inspection area without permission.

5.2.6 DURESS ALARMS

Duress alarms installed at fixed locations (see Figure 5-5) or carried as mobile devices alert security personnel to a potential threat or incident. If used outside a defined area, duress alarms should be programmed to transmit the precise location of the user.

5.2.7 MAIL/PACKAGE SCREENING

Mail and package screening involves controlling and screening the mail and packages for contraband, weapons, chemical, biological, radiological, or incendiary materials, and other items, whether brought into a facility by an individual or by mail/package delivery. Screening technologies may detect components of explosive devices or explosive compounds by radiographic analysis, by analyzing chemical emissions, or by other methods (see Figure 5-6). Radiological detectors, which are accurate,

reliable, and relatively inexpensive, may also be used. Package screening measures may include:

- Arranging for off-site inspection of mail/packages
- Centralizing mail/package delivery and screening into a standalone building or on the perimeter of the facility
- Providing explosive detection and response training to mail handlers
- Conducting X-ray screening of mail and packages
- Utilizing explosive and CBR detection equipment

Figure 5-5: Emergency phone in parking garage.

SOURCE: BOB CIZMADIA

Figure 5-6: Example of an air sampling system in a mailroom.

SOURCE: TERRENCE RYAN

5.3 INTERDICTION/RESPONSE MEASURES

Response/interdiction forces provide a means to delay adversaries while protecting personnel and critical locations from blast and CBR events. Response force requirements are dependent on contingency planning and range from on-site or off-site security guards to local and State police forces. Response/interdiction measures include security guard forces with a deterrence or delay role, security guard forces with a response/interdiction role, and general contingency planning with local and State police.

Security guard services consist of proprietary or contract guards, or a combination of both depending on their purpose, the size of the facility, and other factors. Their effectiveness, however, is dependent on the quality of the individuals involved. Proper licensing, training, and background checks are critical for ensuring each individual response force member is qualified.

5.3.1 GUARD FORCE – DETECTION/DELAY ROLE

Guard forces with a detection or delay role generally monitor video surveillance equipment, check credentials, and patrol. They may be located in a lobby area, a patrol area, or in a security operations center connected to several entry points. These security guards perform access control functions and surveillance by either direct observation or through video surveillance. If an event occurs, they conduct an assessment and coordinate the response actions of employees and internal and external response forces. They may also respond directly to events if simple interdiction may limit the incident or to assist with evacuation and isolation.

For the largest facilities, the security guard may be afforded a protected booth with hardened walls, protected egress, pass tray, access denial system, CCTV monitors, controls of entrances and exits, radios, telephones, paging systems, intercoms, key boxes, indicator and alarm panels, the active vehicle barrier override control, security light controls, elevator controls, and controls for air-handling systems.

5.3.2 GUARD FORCE – RESPONSE/INTERDICTION ROLE

Guard forces with a response/interdiction role are more highly trained and responsible for conducting containment and denial actions. Guards may be trained and equipped for duties including: delaying at a distance, delaying to permit occupants at risk to escape, and finally delay–hold–counterattack. These guards protect personnel, goods, and services, but should not be expected to engage in law enforcement activities.

GUARD FORCE ROLES

- **Detection.** Monitor video surveillance equipment, control access, and patrol to detect threats.
- **Delay at a Distance.** Increase the time that elapses between the detection of an imminent terrorist attack and the actual onset of an attack to permit the arrival of response forces or the successful evacuation of personnel.
- **Delay to Permit Flight.** Increase the amount of time that elapses between the onset of an attack and terrorist access to executives to permit the arrival of response forces or the successful evacuation of executives under attack.
- **Delay, Hold, and Counterattack.** Increase the duration of an attack by allowing occupants to remain secure in a safe haven until a response force can arrive to repulse the attack, and apprehend the terrorists.

5.3.3 RESPONSE FORCE CONTINGENCY PLANNING

Conducting contingency planning and documenting procedures are critical to an effective response function. Contingency planning involves identifying potential intruders and developing response procedures for each likely threat. For example, facilities may specify a level of force that guards would be expected to use in different scenarios. Contingency planning also ensures the availability and redundancy of communication systems with both internal and external responders. This increases the ability of the guards to receive notification of an event, coordinate their internal response, and synchronize the response with outside agencies.

5.4 PROCEDURAL MEASURES

Procedural measures are the policies and procedures that limit vehicle and pedestrian movement around and within critical areas, limit the release of building information, such as plans and schematics, and encourage employee support of security programs. While most commercial buildings need to provide access for their tenants, customers, or the general public, each employee, maintenance person, and visitor does not need equal access to every space. Restricted areas may protect critical infrastructure or simply keep the public in easily observable spaces. Designating and enforcing parking controls are procedural measures of special note because of the possible use of vehicle bombs by terrorists.

5.4.1 RESTRICTED AREAS

Restricted areas are classified as controlled, limited, or exclusion areas, depending on the degree of security and control required (see Figure 5-7).

Figure 5-7: Electronic entry control device into restricted area.
SOURCE: BOB CIZMADIA

Controlled Area. A controlled area is that portion of a restricted area near or surrounding a limited or exclusion area. Entry to a controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled because entry does not provide access to a security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone to the in-depth security of the limited or exclusion area.

Limited Area. A limited area is a restricted area near a security interest. Uncontrolled movement may permit access to the security interest. Escorts and other internal restrictions may prevent access within limited areas.

Exclusion Area. An exclusion area is a restricted area containing a security interest. Uncontrolled movement permits direct access to the security interest.

5.4.2 PARKING AND TRAFFIC CONTROLS

In general, vehicle parking near buildings should be discouraged due to the threat of vehicle bombs. While pre-entry screening of vehicles at perimeter entrances will decrease the risk of penetration by vehicle-borne improvised explosive devices (IED), it does not eliminate this hazard. Restricting unscreened vehicles from parking under facilities, from parking within a predetermined distance from a building, or from traveling into a protected area will increase blast protection.

In summary, parking and traffic control activities include:

- Control on-site parking with ID checks, security personnel, and access systems (see Figure 5-8)
- Separate employee and visitor parking
- Eliminate internal building parking
- Ensure natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities
- Prevent pedestrian access to parking areas other than via established entrances

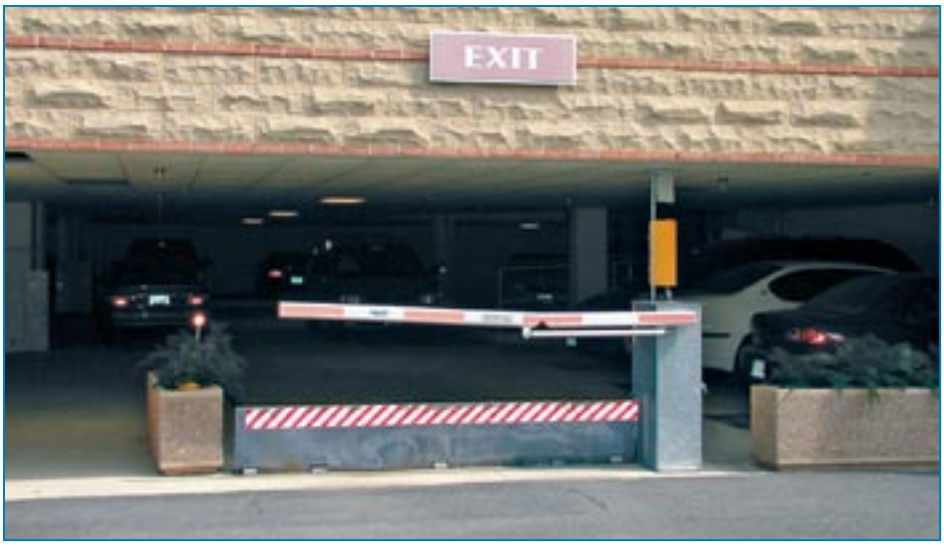

Figure 5-8: Parking control.

SOURCE: TERRENCE RYAN

5.4.3 RESTRICT ACCESS TO FACILITY INFORMATION

Facility information, including drawings and operational procedures for mechanical, electrical, plumbing, structural, and security systems should be controlled, and its release should be restricted.

5.4.4 ENCOURAGE EMPLOYEE SUPPORT

Procedural measures require that employees be motivated to support the security program. Regardless of the security measures employed, if employees do not follow operational policies and procedures, vulnerabilities will persist. An appropriate corporate climate, adequate operational planning, and established management objectives will help encourage employees to support security measures.

5.5 PREPAREDNESS MEASURES

Preparedness measures are actions taken to increase readiness for a crisis, mitigate impacts, and respond to and recover from an incident. These include disaster preparedness planning, conducting risk assessments, developing mass notification warning systems, evacuation planning, preparing to shelter in place, monitoring systems and resources, and conducting training exercises.

PREPAREDNESS MEASURES

- Develop a Disaster Preparedness Plan
- Conduct Risk Assessments
- Develop Mass Notification Systems
- Conduct Evacuation Planning and Shelter in Place Preparation
- Monitor Systems and Resources
- Conduct Training Drills and Exercises

More information on disaster preparedness is available at the FEMA Web site: www.fema.gov/plan/index.shtm

5.5.1 DEVELOP A DISASTER PREPAREDNESS PLAN

Protecting facilities begins with developing a disaster preparedness plan. The FEMA Web site provides numerous links and examples of plans that can be tailored to fit your facility. The risk assessment, as well as identification of mitigation measures to minimize or prevent losses, provides the basis for developing the plan.

5.5.2 CONDUCT RISK ASSESSMENTS

Risk assessments are conducted to assess threat/hazards, impacts on assets, vulnerabilities to incidents, and subsequent risks. Security countermeasures should be defined and prioritized relative to their impact on risk.

5.5.3 DEVELOP MASS NOTIFICATION SYSTEMS

Mass notification systems, such as automatic messaging or public address systems, should be developed to reach all building occupants. These systems should provide warning and alert information, along with actions to take before and after an incident. System and electric power redundancy should be ensured.

5.5.4 EVACUATION PLANNING AND SHELTER IN PLACE PREPARATION

The building occupants should be prepared for independent action prior to the arrival of emergency responders. This preparation involves evacuation planning and shelter in place preparation. The building occupants should also be trained on the Incident Command System in order to understand the chain of command, available integrated communications, and management of resources throughout the recovery.

5.5.5 MONITOR EMERGENCY SYSTEMS AND RESOURCES

Systems and resources intended to support the facility during a crisis should be monitored to ensure their availability and function. Examples of such systems and resources include, but are not limited to:

- Emergency equipment and critical utilities
- Fire alarms and detection and suppression systems
- Emergency resources and vendors (e.g., fuel for emergency generators)
- Alternate worksites
- Updated maps and floor plans
- System backups and off-site storage

5.5.6 CONDUCT TRAINING DRILLS AND EXERCISES

Training drills and exercises help to improve efficiency of emergency response teams and employees, clarify responsibilities, reveal weaknesses, and reduce stress. A commitment to testing also lends credibility and authority to the security program.

In summary, training involves:

- Rehearsing emergency plans with local law enforcement
- Conducting joint exercises with first responders

EMERGENCY MANAGEMENT

Complete information on the management of various emergency events and the Incident Command System is available from the FEMA Web site: www.fema.gov/emergency/nims/index.shtm

5.6 SECURITY MASTER PLANNING

All of these operational security measures should be guided by the final component, a Security Master Plan (see Figure 5-9). This 3- to 5-year plan, based on the goals of the overall organization, states the vision, goals, and objectives of the security program. The plan should also outline the operational security measures, the path for the security program to keep pace with the changing threat environment, and future initiatives. Further, it should be integrated into the organization's facility planning process as well as benchmarked against the security programs of similar facilities.

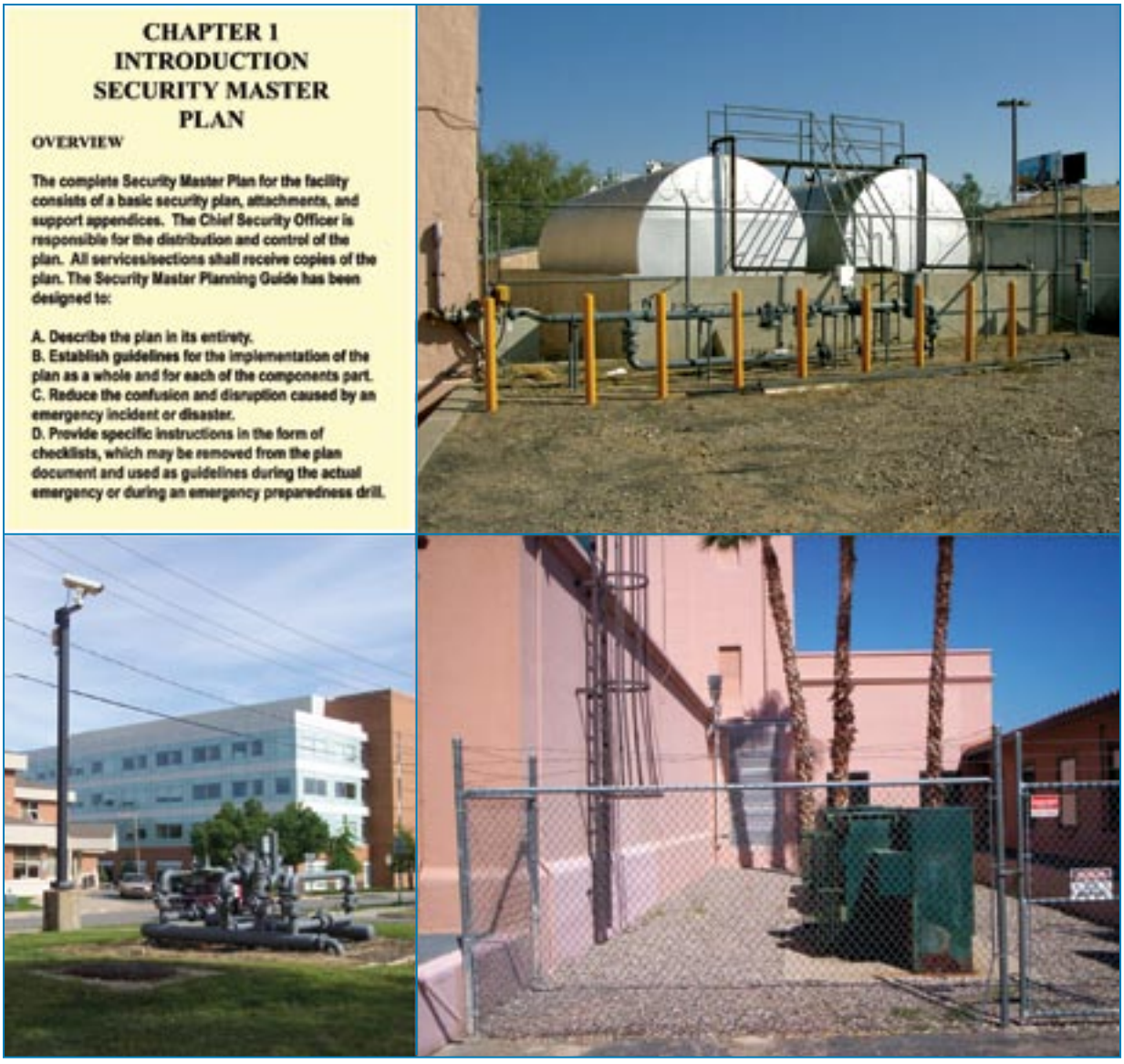

Figure 5-9: Security Master Planning integrates the operational security measures into the organization's facility planning process. SOURCE: TERRENCE RYAN

A comprehensive Security Master Plan should:

- Be communicated and disseminated to all levels of management and building occupants as appropriate
- Be integrated into the facility construction or renovation planning
- Be benchmarked or compared to related facilities
- Be tested and evaluated
- Identify threats/hazards, assets, vulnerabilities, and risks
- Establish a security improvement implementation schedule
- Establish a security operating and capital budget
- Follow regulatory or industry guidelines/standards

5.7 ADDITIONAL ASPECTS OF OPERATIONAL SECURITY MEASURES RELATED TO BLAST EVENTS

Tactics for developing and employing IEDs are continuing to evolve. Fortunately, responses to IED threats are also rapidly changing as technologies and procedures to detect and mitigate the terrorist leave-behind IED, human-carried IED, and vehicle-borne IED threats progress. Evolving countermeasure technologies are designed to provide time-sensitive information that security forces, critical asset managers, police/bomb squads, and incident commanders need to detect and counter IEDs away from critical infrastructure and personnel.

Additional operational security measures related to blast events include establishing an explosive detection program, establishing bomb threat procedures, and establishing blast-related mail/package handling procedures.

ADDITIONAL OPERATIONAL SECURITY MEASURES FOCUSED ON BLAST EVENTS

- Establish an explosive detection program
- Establish bomb threat procedures
- Establish blast-related mail/package handling procedures

5.7.1 ESTABLISH AN EXPLOSIVE DETECTION PROGRAM

The effectiveness of an explosive detection program is dependent on the level of sophistication of the detection measures. At the low end, bomb detection is conducted by inspection. Higher levels of protection are achieved using detection equipment, such as X-ray devices, metal detectors, and explosive detectors. Explosive detection dogs are an alternative to explosive detection technology.

5.7.2 ESTABLISH BOMB THREAT PROCEDURES

The following procedures should be followed when receiving a telephoned bomb threat:

- Get as much information from the caller as possible. Ask the following questions, if possible:

  When is the bomb going to explode?

  Where is it right now?

  What does it look like?

  What kind of bomb is it?

  What will cause it to explode?

  Did you place the bomb?

  Why?

  What is your address?

  What is your name?

- Keep the caller on the line and record the conversation.

- Notify the police and building management.

5.7.3 ESTABLISH BLAST-RELATED MAIL/PACKAGE HANDLING PROCEDURES

Over the years, postal inspectors have identified typical characteristics of suspicious parcels. In many cases the packages:

- Are unexpected or from someone unfamiliar

- Have no return address or have one that cannot be verified as legitimate
- Have protruding wires or aluminum foil, strange odors, or stains
- Show a city or State in the postmark that doesn't match the return address
- Are of unusual weight given their size or are lopsided or oddly shaped
- Are marked with threatening language
- Have inappropriate or unusual labeling
- Have excessive postage or packaging material, such as masking tape and string
- Have misspellings of common words
- Are addressed to someone no longer with your organization or are otherwise outdated
- Have incorrect titles or titles without a name
- Are not addressed to a specific person
- Have hand-written or poorly typed addresses

5.8 ADDITIONAL ASPECTS OF OPERATIONAL SECURITY MEASURES RELATED TO CBR EVENTS

When protecting and responding to an accidental hazardous material release or an intentional CBR attack on a commercial building, focus operational security measures on personnel and vehicle access points, storage areas, the roof, mechanical areas, outdoor air intakes, and water utility feeds. The operational security needs of each building should be individually assessed, as the threat from a nearby hazardous material release or an actual CBR attack will vary considerably from building to building (Figure 5-10). Some operational security measures are low cost, such as locking doors to mechanical rooms or water utility pits, and can be implemented in retail, office, and multifamily residential buildings. Other operational security measures, such as personnel and package searches by X-ray or explosive detection

equipment, are expensive and may substantially inconvenience businesses. Measures should be implemented as warranted after careful consideration of the likelihood of an incident and the resulting consequences.

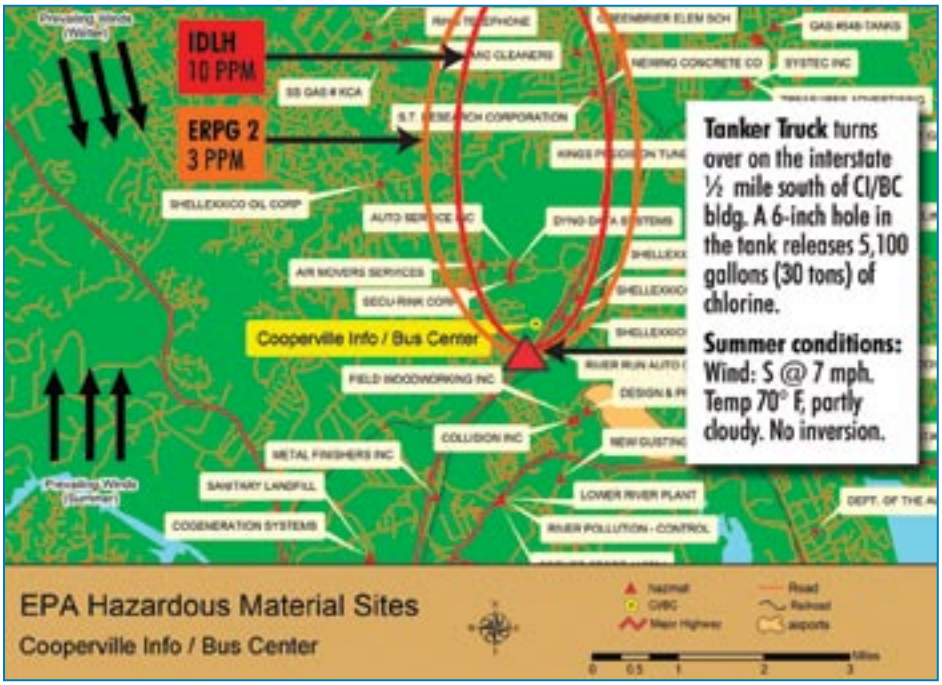

Figure 5-10: Projected plumes of CBR incident.

SOURCE: MICHAEL KAMINSKAS

ADDITIONAL OPERATIONAL SECURITY MEASURES FOCUSED ON CBR EVENTS

- Restrict access, and secure and monitor outdoor air intakes
- Light, secure, and monitor utility access points
- Secure and monitor exterior mechanical/electrical spaces
- Secure and monitor interior HVAC access points
- Provide internal first responders appropriate hazardous materials equipment
- Restrict access to facility and utility drawings
- Prevent unauthorized access and monitor roof areas
- Establish CBR related mail/package handling procedures

5.8.1 PREVENT ACCESS, AND SECURE AND MONITOR OUTDOOR AIR INTAKES

A contaminant could quickly spread throughout the building by the HVAC system. Air intakes that are publicly accessible and at or below ground level are at the most risk due to ease of approach, as well as characteristics of many CBR agents that cause them to remain close to the ground. Relocating or extending the air intakes upward can prevent access. Creating a restricted area to prevent public access, but allow access for authorized personnel can also improve security. Fencing or similar see-through barriers are preferred to allow visual detection of abnormal activity or a deposited CBR source. Security lighting should be provided for outdoor air intakes and other accessible points of the HVAC system, which should also be monitored with CCTV cameras. Intrusion detection sensors programmed to activate alarms, redirect surveillance cameras, and initiate recording should also be installed.

5.8.2 ESTABLISH CBR-RELATED MAIL/PACKAGE HANDLING PROCEDURES

Additional measures to mitigate the dangers from suspicious envelopes and packages with potential CBR agents include:

- Refraining from eating or drinking in a designated mail handling area
- Placing suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents
- Avoiding sniffing or smelling suspect mail
- Covering the envelope or package with anything available (e.g., clothing, paper, or trash can)
- Leaving the room and closing the door and/or sectioning off the area to prevent others from entering
- Washing your hands with soap and water to prevent spreading any contaminants to your face
- Reporting the incident to your building security official or an available supervisor, who will notify authorities without delay
- Listing all people who were in the room or area when this suspicious letter or package was recognized to help local public health

authorities and law enforcement officials with follow-up investigations and advice

5.8.3 ADDITIONAL MEASURES

Additional measures to mitigate the potential spread of CBR agents through plumbing, mechanical, and electrical systems include:

- Hardening and locking incoming water service line junction points and service pits by installing intrusion detection sensors on the access points for all site utilities.

- Providing security lighting and monitoring on-site stored water and associated junction points with CCTV systems (Figure 5-11).

Figure 5-11: Exterior video camera for monitoring critical utilities.

SOURCE: BOB CIZMADIA

- Conducting perimeter surveys to identify mechanical, plumbing, and electrical rooms with exterior doors, windows, and utility openings. Hardening and locking the doors. Providing grills or louvers for all windows and man-passable openings in exterior walls below the second floor. (Openings greater then 96 square inches are considered man-passable.) Installing intrusion detection sensors on the access points.

- Securing exterior mechanical spaces and equipment. Identifying external mechanical spaces and equipment that are publicly accessible and establishing a means for direct surveillance, or monitoring with intrusion detection equipment and CCTV systems.

- Securing interior HVAC access points, such as return-air grills. Identifying the return-air grills that are publicly accessible and establishing a means for direct surveillance, or monitoring with intrusion detection equipment and CCTV systems. Removing or relocating furniture that obscures surveillance or provides access to the return air grills.

- Providing internal first responders access to appropriate hazardous materials response equipment. Required items, such as a hazardous material suit, gloves, boots, and a protective hood, may be packaged together for convenience.

- Restricting access to mechanical, plumbing, and electrical systems by outside maintenance personnel. Providing escorts for outside maintenance personnel that have not been pre-screened or are not from a trusted provider.

- Restricting access to facility and utility drawings and schematics.

- Preventing unauthorized access and monitoring facility roofs, which can provide access to HVAC systems, air intakes, and exhaust vents. Establishing fencing or barriers to restrict access from adjacent roofs. Locking and monitoring roof access doorways. Providing grills or louvers to man-accessible openings.

5.9 PRIORITIZATION OF OPERATIONAL SECURITY CONSIDERATIONS

Commercial buildings range in function from retail to office to multi-family facilities and hotels. They can be free-standing, strip mall, or multi-story structures, and have one occupant or thousands. These characteristics vary depending on whether building is located in a rural setting, a suburban setting, or a large urban area. The following general guidance is provided to protect retail, office, and multi-family apartment buildings, and hotels.

5.9.1 RETAIL BUILDINGS

Retail buildings are openly accessible to the public. This limits some of the operational physical security measures that can be applied. Physical hardening of the critical infrastructure may be implemented to address this limitation. However, even in these buildings, operational security measures can be applied:

- Restricted areas can be established for mechanical rooms, loading docks, roofs, and air vents.
- Interior and exterior CCTV systems may be established both for loss prevention and security detection.
- Anti-ram, landscaping, and other vehicle barriers may be established to mitigate the vehicle-borne IED threat.
- Certain detection and delay measures, such as visitor screening and access control, may not be practical during business hours. However, after business hours, all intrusion detection measures can be activated.
- Most procedural, preparedness, and master planning measures can be applied. Of these, rehearsing emergency plans with local law enforcement and conducting joint exercises with first responders are especially important because they contribute to a coordinated response in an incident.

5.9.2 OFFICE BUILDINGS

Office buildings usually have a circulation plan and procedures that permit greater control over visitors compared to retail facilities. This facilitates the use of the full range of the operational security measures to protect offices from blast and CBR attacks. Based on the risk assessment for an office building, effective physical security measures to deter, delay, detect, and interdict/respond may be established. All procedural, preparedness, and master planning measures, as appropriate, may also be applied.

5.9.3 MULTI-FAMILY APARTMENT BUILDINGS

A range of operational security measures is available for use in multi-family apartment buildings. Emergency preparedness plans and occupant

education may be the most important life savers in the event of an attack. Measures should include:

- Reviewing and updating emergency preparedness plans
- Providing education and training to occupants on evacuation procedures and identifying and reporting suspicious activity

Installing suitable hardware to lock doors and windows (delay measures) and using a remotely monitored alarm system (detection and interdiction/response measures) may also be useful in rented or leased spaces.

5.9.4 HOTEL SECURITY MEASURES

Operational security measures, similar to those for the other types of commercial buildings, may be established to protect a hotel from blast- and CBR-related events. Interior and exterior video surveillance systems may be established for loss prevention and security detection. Access to mechanical rooms, loading docks, roofs, and air vents should be restricted. Visitor screening and access control can be established during nighttime hours.

Most procedural, preparedness, and master planning measures can also be applied. Of these, rehearsing internal emergency plans and establishing a liaison with local law enforcement and other first responders are especially important because they contribute to a coordinated response in an incident.

5.10 INCREMENTAL INTEGRATION OF OPERATIONAL AND PHYSICAL SECURITY MEASURES INTO A RISK REDUCTION PROGRAM: FLEXIBILITY AND TRADEOFFS

Providing both an open, business-friendly environment and a safe and secure facility involves a delicate balance. Many diverse technologies are available to meet the security needs of a specific facility. The following flexibility and tradeoff considerations will help in the selection of incremental operational security measures.

Balance program improvements. Incremental increases in security should be implemented program-wide, with balanced deterrence, delay, detection and assessment, and interdiction/response measures.

Randomly implemented technology may only have a limited impact on risk reduction. For example, establishing electronic security systems on the doors and not the windows of a facility does not significantly improve security. Similarly, establishing a hardened, gated vehicle entrance that can be bypassed by driving across a lawn does not appreciably improve protection from vehicle bombs. Facility owners should plan incremental improvements that decrease the level of risk and increase the overall level of protection.

Use technology to improve detection effectiveness. Having a guard watching a bank of CCTV monitors without technology cueing systems usually limits detection. The integration of sensors with a CCTV system greatly increases the security effectiveness and the area that can be covered. Replacing or supplementing security guards with centralized monitoring station technology, rather then adding more personnel to monitor simple CCTV systems, may be a cost-effective incremental improvement.

Internet Protocol (IP)-based systems may provide flexibility and eliminate the need to integrate with other renovation projects. The rapid shift away from the classic, analog-only CCTV solutions to digital encoding and IP or network transport over open system connections presents existing building owners with new improvement opportunities. The installation of IP-based electronic security systems does not require the disruptive installation of long individual cable runs back to a central console. IP-based systems can generally be installed independent of major facility renovations.

Wireless systems may increase flexibility. In the past, installation of traditional wired external cameras or intrusion detection systems required thousands of dollars in installation costs and business disruptions from digging up roadways or parking lots to bury cables. This type of improvement had to be linked to other scheduled major renovations. Now, with IP-based systems and wireless links, installation may be less expensive and less disruptive, and can be completed independent of other scheduled renovations. However, wireless systems are more accessible to outsiders than wired systems and require appropriate protection, such as encryption, firewalls, and passwords to prevent hacking and tampering.

Not all hardware and software applications are compatible. Many proprietary systems cannot be integrated with other systems. They may also preclude future upgrades or the introduction of new capabilities. Facility managers should carefully project requirements and the necessary components of a complete system and plan for incremental improvements accordingly.

Plan the implementation of variable security measures. After establishing a baseline of protection, facility managers must be able to increase their protective posture in response to an increased threat. While many physical measures have long lead times (like applying fragment retention film on windows), many operational security measures do not require major capital improvement and can be quickly modified as needed. The practiced and proven capability to implement variable security measures, such as closing underground parking, screening visitors, or limiting access, may provide facilities with the alternative of continuing operations rather than doing nothing or closing during periods of increased threat.

Install a high profile security measure early in the improvement sequence to publicly highlight increased security. If a facility has several equally effective improvements, schedule the high profile items, such as gated entry into the loading dock area or a public access control system, early to increase the public perception of security.

5.11 OPERATIONAL SECURITY PROTECTION MEASURES

The operational security measures identified in the preceding discussions are listed below as an example of measures that might be generated by the FEMA 452 process and implemented using this document, as discussed in Chapter 2. The measures are categorized into those that include physical protection and strengthening measures (5.11.1), and those that are entirely operational (5.11.2). The former are all included in the list that comprises the vertical axes of the matrices in Section 2.3.

5.11.1 PHYSICAL PROTECTION AND STRENGTHENING BUILDINGS

1. Operational security measures related to blast and CBR events
    - ❍ Detection and assessment measures
        - ❍ Exterior intrusion detection systems
        - ❍ Interior intrusion detection systems
        - ❍ Video assessment and surveillance systems
        - ❍ Access control systems
        - ❍ Duress alarms

- Interdiction/response measures
  - Guard force: detection/delay role

2. Additional operational security measures related to blast events
   - None.

3. Additional operational security measures related to CBR Events
   - Restrict access and secure and monitor outdoor air intakes
   - Light, secure, and monitor water service access points
   - Install intrusion detection sensors for all utility services to the building
   - Secure and monitor exterior mechanical spaces and equipment
   - Secure and monitor interior HVAC access points

These measures can be implemented independently from one another.

5.11.2 OPERATIONAL MEASURES

1. Operational security measures related to blast and CBR events
   - Detection and assessment measures
     - Exterior intrusion detection systems
     - Interior intrusion detection systems
     - Video assessment and surveillance systems
     - Access control systems
     - Vehicle inspection systems
     - Duress alarms
     - Mail/package screening procedures
   - Interdiction/response measures
     - Guard force: detection/delay role
     - Guard force: response/interdiction role
     - Response force contingency planning
   - Procedural measures

- Restricted areas: controlled areas
- Restricted areas: limited areas
- Restricted areas: exclusion areas
- Parking and traffic controls: separate employee and visitor parking
- Parking and traffic controls: eliminate internal building parking
- Parking and traffic controls: ensure natural surveillance
- Parking and traffic controls: limit pedestrian access to parking areas
- Restrict access to facility information
- Encourage employee support

- Preparedness measures
  - Develop a disaster preparedness plan
  - Conduct risk assessments
  - Develop mass notification systems
  - Conduct evacuation planning and shelter in place preparation
  - Monitor emergency systems and resources
  - Conduct training drills and exercises
- Security master planning measures
  - Communicate and disseminate security master plan
  - Integrate into the facility construction or renovation planning
  - Benchmark or compare to related facilities
  - Test and evaluate the plan
  - Identify threats/hazards, assets, vulnerabilities, and risks
  - Establish security improvement implementation schedule
  - Establish security operating and capital budget

2. Additional operational security measures related to blast events
   - Establish an explosive detection program
   - Establish bomb threat procedures

- Establish mail/package handling procedures

3. Additional operational security measures related to CBR events
   - Restrict access to, secure, and monitor outdoor air intakes
   - Light, secure, and monitor water service access points
   - Install intrusion detection sensors for all utility services to the building
   - Secure and monitor exterior mechanical spaces and equipment
   - Secure and monitor interior HVAC access points
   - Provide first responders appropriate hazardous materials equipment
   - Restrict access to critical utility drawings
   - Prevent unauthorized access to and monitor roof areas
   - Establish CBR-related mail/package handling procedures

All of these measures can be implemented independently from one another.

5.11.3 OPERATIONAL MEASURES CATEGORIZED INTO THE BUILDING VULNERABILITY ASSESSMENT CHECKLIST

The following list of operational mitigation measures reorganizes the preceding list (5.11.2) into the 13 sections of the Building Vulnerability Assessment Checklist in Appendix A of FEMA 452. Where applicable, the references in parentheses below refer to the respective sections in Chapters 4 and 5 where the item is discussed.

1. Site

   1.1 Vehicle inspections (5.2.5)

   1.2 Guard force, detection/delay role (5.3.1)

   1.3 Guard force, response/interdiction role (5.3.2)

   1.4 Parking and traffic controls (5.4.2)

   1.4.1 Control on-site parking

1.4.2 Separate employee and visitor parking

1.4.3 Eliminate internal building parking

1.4.4 Ensure natural surveillance

1.4.5 Limit pedestrian access to parking areas

2. Architectural

2.1 Expedient sheltering in place (4.4.1.2)

2.1.1 Designating safe rooms, interior rooms having a lower air exchange rate

2.1.2 Identifying switches for all air handling units and fans for deactivation

2.1.3 Defining procedures for sheltering and for purging the building after plume passage

2.1.4 Establishing a building-wide notification system

2.1.5 Familiarizing occupants with the procedures and responsibilities

2.2 Evacuation (4.4.1.2)

2.3 Using escape respirators (4.4.1.2)

2.4 Enhanced physical security (4.4.2.2)

2.4.1 Perform entry inspections

2.4.2 Employ video surveillance equipment

2.4.3 Institute mail screening procedures

2.4.4 Maintain operational security to building plans and signage

2.5 Mail/package screening (5.7.3, 5.8.2)

2.6 Restricted areas (5.4.1)

2.6.1 Controlled areas

2.6.2 Limited areas

2.6.3 Exclusion areas

2.7 Prevent unauthorized access to and monitor roof areas (5.8.4)

3. Structural Systems

4. Building Envelope

5. Utility Systems (water, sewer, fuel, electrical service, telephone, fire alarm)

6. Mechanical Systems (HVAC)

6.1 Purging (expedient sheltering in place (4.4.1.2))

7. Plumbing and Gas Systems

8. Electrical Systems

9. Fire Alarm Systems

10. Communications and Information Technology Systems

10.1 Expedient sheltering in place

10.1.1 Defining building-wide notification system

10.2 Develop mass notification systems (5.5.3)

11. Equipment Operations and Maintenance

11.1 Provide first responders appropriate hazardous materials equipment (5.8.4)

12. Security Systems (perimeter security, interior security, security system documents)

13. Security Master Plan

13.1 Detection and assessment measures

13.1.1 Vehicle inspection systems (5.2.5)

13.1.2 Mail/package screening procedures (5.2.7)

13.2 Interdiction/response measures

13.2.1 Response force contingency planning (5.3.3)

13.3 Procedural measures

13.3.1 Restrict access to facility information (5.4.3)

13.3.2 Encourage employee support (5.4.4)

13.4 Preparedness measures

13.4.1 Develop disaster preparedness plan (5.5.1)

13.4.2 Conduct risk assessments (5.5.2)

13.4.3 Conduct evacuation planning and shelter in place preparation (5.5.4)

13.4.4 Monitor emergency systems and resources (5.5.5)

13.4.5 Conduct training drills and exercises (5.5.6)

13.5 Security master planning measures (5.6)

13.5.1 Communicate and disseminate

13.5.2 Integrate into the facility construction or renovation planning

13.5.3 Benchmark or compare to related facilities

13.5.4 Test and evaluate the plan

13.5.5 Identify threats/hazards, assets, vulnerabilities, and risks

13.5.6 Establish security improvement implementation schedule

13.5.7 Establish security operating and capital budget

13.6 Additional operational security measures related to blast events

13.6.1 Establish an explosive detection program (5.7.1)

13.6.2 Establish bomb threat procedures (5.7.2)

13.6.3 Establish mail/package handling procedures (5.7.3)

13.7 Additional operational security measures related to CBR events

13.7.1 Restrict access to critical utility drawings (5.8.4)

These security enhancement operational increments can be implemented at any time, as they do not entail physical work in the building.