**Healthcare Facility Security Assessment Instrument (Date: \_\_\_\_\_)**

**Name and Image of Facility**

**Facility:** **# and type beds**

***This document has been prepared for***

***and is confidential pursuant to Florida Statute 395.1056***



**The Healthcare Facility Security and Vulnerability Assessment Instrument was developed for the Bureau of Preparedness and Response, Division of Emergency Preparedness and Community Response, Florida Department of Health by the O’Gara Group, Training and Services Division under contract to the Florida Department of Health. Funding for this contract was provided by the National Bioterrorism Hospital Preparedness Program, CFDA 93.889.**

**The purpose of this Healthcare Facility Security and Vulnerability Assessment Instrument is to: (1) identify a facility’s protective measures and vulnerabilities that may be exploited by an adversary to degrade the facility’s ability to carry out its mission (2) identify the vulnerabilities of the facility’s physical attributes that may enable a manmade or naturally occurring disaster to degrade the facility’s ability to carry out its mission and (3) provide information to enhance a facilities protective measures and mitigate it’s vulnerabilities.**

Table of Contents

[I. Facility Profile 4](#_Toc278793155)

[Community Profile 5](#_Toc278793156)

[II. Commendable Actions 7](#_Toc278793157)

[III. Recognizability 8](#_Toc278793158)

[Options for Consideration – Recognizability 8](#_Toc278793159)

[IV. Perimeter Access Control 9](#_Toc278793160)

[Options for Consideration – Perimeter Access Control 10](#_Toc278793161)

[V. Proximity/Stand-Off 11](#_Toc278793162)

[Options for Consideration – Proximity/Standoff 12](#_Toc278793163)

[VI. Lighting 13](#_Toc278793164)

[Options for Consideration – Lighting 14](#_Toc278793165)

[VII. Signage 15](#_Toc278793166)

[Options for Consideration – Signage 16](#_Toc278793167)

[VIII. Ingress/Egress 17](#_Toc278793168)

[Options for Consideration – Ingress/Egress 18](#_Toc278793169)

[IX. Parking 19](#_Toc278793170)

[Options for Consideration – Parking 19](#_Toc278793171)

[X. Surveillance 21](#_Toc278793172)

[Options for Consideration – Surveillance (EXTERNAL) 22](#_Toc278793173)

[XI. Security Measures 23](#_Toc278793174)

[Options for Consideration – Security Measures 24](#_Toc278793175)

[XII. Personnel 25](#_Toc278793176)

[Options for Consideration – Personnel 25](#_Toc278793177)

[XIII. Interior Access Control 27](#_Toc278793178)

[Options for Consideration – Interior Access Control 29](#_Toc278793179)

[XIV. Alarms & Sensors 30](#_Toc278793180)

[Options for Consideration – Alarms & Sensors 31](#_Toc278793181)

[XV. Video Surveillance 32](#_Toc278793182)

[Options for Consideration – Video Surveillance 33](#_Toc278793183)

[XVI. Communications 34](#_Toc278793184)

[Options for Consideration – Communications 35](#_Toc278793185)

[XVII. Critical Nodes 36](#_Toc278793186)

[Options for Consideration – Critical Nodes – Chillers 40](#_Toc278793187)

[XVIII. Utilities 41](#_Toc278793188)

[XIX. HVAC 46](#_Toc278793189)

[Options for Consideration – HVAC 47](#_Toc278793190)

[XX. HazMat 48](#_Toc278793191)

[Options for Consideration – Hazmat 49](#_Toc278793192)

[XXI. Interdependencies 50](#_Toc278793193)

[XXII. Dependencies 51](#_Toc278793194)

[XXIII. Food Handling 52](#_Toc278793195)

[XXIV. Delivery Procedures [Loading Dock & Mailroom] 53](#_Toc278793196)

[Options for Consideration – Delivery Procedures (Loading Dock and Mailroom) 54](#_Toc278793197)

[XXV. Other Consideration 55](#_Toc278793198)

[Elevators 55](#_Toc278793199)

[Windows 56](#_Toc278793200)

[Pharmacy: 57](#_Toc278793201)

[Options for Consideration – Pharmacy 58](#_Toc278793202)

[Plans and Procedures 58](#_Toc278793203)

[Options for Consideration – Plans and Procedures 59](#_Toc278793204)

[Fire Suppression 59](#_Toc278793205)

[Non-Agency Tenants 60](#_Toc278793206)

[Special Events 61](#_Toc278793207)

[Helipad 61](#_Toc278793208)

[Newborn/Pediatrics 61](#_Toc278793209)

[XXVI. References 62](#_Toc278793210)

[XXVII. Glossary of Terms & Acronyms 63](#_Toc278793211)

[Appendix A – Instructions for Assessors 65](#_Toc278793212)

[Appendix B – Options for Consideration Summary 68](#_Toc278793213)

# I. Facility Profile

Facility Legal Name .

Facility Common/Local Name (if different) .

Facility Address .

County .

GPS Latitude / Longitude .

Elevation .

Storm Surge/Flood Zone Designation (*what is their zone designation? ex: A, B, C, or minimum, maximum*) .

Facility Phone Number .

Facility Website .

Campus Acreage/Area .

Number of Buildings

Facility Size .

Average # Staff Onsite Daily .

Average # Visitors/Patients Onsite Daily .

Construction Type .

Exterior Wall Color .

Critical Infrastructure .

Primary Ingress/Egress Routes .

Any new construction or planned building .

###### Emergency Contact Information (Primary)

Name .

24/7 Phone .

Email .

###### Primary Assessor

Assessor’s Name

Assessor’s Agency

Assessor’s Phone Number

Assessor’s Email Address

## Community Profile

Guidance:

Adjacent land uses and occupancies could be used to facilitate attacks on this asset, and maybe potential targets themselves, present collateral damage or cascading failure hazards. It is important to identify the types of property, buildings, and activities adjacent to and in proximity of this facility?

The site analysis represents the first step of security defense planning, which considers the site perimeter and grounds. Site design measures can include walls, heavy plantings, fences, berms, ditches, lighting, and natural topographic separations. The following are questions to ask at this stage:

The basis of Crime Prevention Through Environmental Design (CPTED) is that proper design and effective use of the built environment can reduce the incidence and fear and opportunity of predatory stranger-to-stranger crime. This in turn leads to improvements in the quality of life (where we live, work, and play). In contrast to the approach of addressing crime concerns by implementing visually affronting security or target hardening measures such as locks, hard barriers, security gates, security patrols, etc., CPTED promotes high quality and visually pleasing solutions as first responses that aim to enhance the legitimate use of space. CPTED can be applied without interfering with the normal use of the space. It is easy to apply and can be economical to implement, especially if it is done early at the planning and design stages of a project.

The Principles of CPTED are:

* Natural Surveillance
* Natural Access Control
* Territorial Reinforcement

●**Natural surveillance.** Increasing visibility by occupants and casual observers increases the detection of trespassers or misconduct at a facility. For instance, if a high wooden fence blocks the view of a loading dock, the lack of visibility may invite thieves. Conversely, the use of chain-link fencing that allows an unobstructed view of the area by workers or passers-by may discourage thieves. Windows, door viewers, mirrors, and other design feature that improve visibility fall under natural surveillance.

●**Natural access control.** The idea is to employ both real and symbolic barriers—including doors, fences, and shrubbery—to define and limit access to a building or other space. For example, to deter burglars from entering lower-story windows, one could plant dense, thorny bushes near the windows or install window locking devices or an alarm system.

●**Natural territorial reinforcement.** This is the process of establishing a sense of ownership, responsibility, and accountability in property owners, managers, or occupants to increase vigilance in identifying trespassers. For example, the use of small edging shrubbery along sidewalks in an apartment complex marks the territory of individual apartments and discourages trespassers from cutting through. Also, people pay more attention to and defend a particular space if they feel psychological ownership of it. Territorial reinforcement measures, which may be physical or symbolic, tell people they are in a defined space. Color, texture, surface variations, signage, and way finding systems are all part of territoriality and boundary setting. Thus, it is possible, through real barriers (fences and walls) and symbolic markers (warning signage, low hedges, low wood picket fences) to encourage tenants or employees to defend the property from individuals with undesirable intentions. Such reinforcement is termed natural because it results from normal, routine use of the environment.

References:

NFPA 730 Guide for Premises Security. National Fire Protection Association. Chapter 5, Security Threat Assessment. Quincy, MA. 2006 Edition, 2010 update. What part of the code applies?

NFPA 101 Life Safety Code. National Fire Protection Association, Chapter 4 – General, Chapter 5 – Performance Based Operations, Chapter 18 – New Health Care Occupancies, Chapter 19 – Existing Health Care Occupancies, Chapter 20 – New Ambulatory Health Care Occupancies, and Chapter 21 – Existing Ambulatory Health Care Occupancies. Quincy, MA. 2009 Edition.

National Institute for Occupational Safety and Health, (NIOSH) Department of Health and Human Services. *Guidance to Protecting Building Environments from Airborne Chemical, Biological or Radiological Attacks*. Centers for Disease Control and Prevention. Cincinnati, OH. May 2002.

Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Chapter 1 “What, Me Worry?”, Chapter 2 “Getting Started”. CRC Press; Boca Raton, Florida. 2008.

Questions:

(Answer these questions below for each side in the Side Specific Description, in a descriptive, narrative form)

* Provide a brief description of the community outside of the asset perimeter? (commercial, industrial, residential, multi-story, single-story buildings, etc.)
* What bodies of water, airports, railroads, streets, major freeway access are near to the facility?
* Are there any adjacent facilities that if damaged/destroyed would cause a degradation of critical services or would create possible hazardous conditions?

Side Specific Description:

Side A: South

Side B: West

Side C: North

Side D: East

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# II. Commendable Actions

Guidance:

Briefly list any noticeable areas that demonstrate proper application of the facility’s security “best practices”?

Identified Commendable Actions:

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# III. Recognizability

Guidance:

Recognizability is the degree to which the asset can be recognized without confusion with other assets or components. Factors that influence recognizability include the size and complexity of the asset, the existence of distinctive asset signatures that clearly identify the type/mission of facility, and the technical sophistication and training of any person(s) who may be planning an attack.

The image of the facility, its grounds, and its staff as clean and well maintained, well managed, organized, and following established national and industry standards of care empowers a facility to be well cared for and more difficult for personnel to engage in acts of criminal behavior without drawing unwanted attention and notice to themselves.

Questions: (Answer these questions in a descriptive, narrative form.)

* What factors make your facility easier to recognize to a possible attacker (e.g., signage, iconic importance to local community, purpose or mission, unique physical/architectural characteristics, etc.)
* What publicly available website sources, facility diagrams, and floor plans could be used to provide intelligence on this facility? (e.g., Google Earth w/Street View, facility site plans/schematics, asset marketing materials)
* Are there any highly recognizable asset features that would present a more likely target to an attacker?

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | . |

Options for Consideration – Recognizability

* Use the “Insert Endnote” button in the “Footnotes” section of the “References” menu tab (Word 2007-2010) to sequentially number this option for consideration.[[1]](#endnote-1)
* Use the copy or keyboard shortcut Ctrl+C to copy you option to reduce duplicative data entry.[[2]](#endnote-2)
* If bullet formatting carries over to the footnote page, use the “Show/Hide” tool to insure that you are selecting only the text and punctuation marks of the option. Any paragraph symbols in your copy selection will for bullet formatting in the footnote.[[3]](#endnote-3)
* Double click on the Endnote citation number in the document or on the Options for Consideration Summary page to toggle between the pages.[[4]](#endnote-4)

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# IV. Perimeter Access Control

Guidance:

Well defined boundaries between public and private areas can be achieved by using physical elements such as fences, architectural design and water features, pavement treatment, art, signage, and landscaping to express ownership, and reinforce territorial boundaries. Identifying intruders is much easier in well-defined spaces. The proper application of these types of items can achieve measures of perimeter access control by incorporating deterrence and delay into the security design.

A security program for a healthcare facility should be designed to protect its tangible assets, such as its workers, patients, information and property. Protection for perimeter areas includes CPTED measures can discourage unauthorized access to the facility and may deter the opportunistic criminal, as well as the determined adversary. Landscaping should be designed and maintained to provide open natural surveillance of the property.

Perimeter access control should be in place in these areas:

* all entrances and exits to the site and building
* perimeter access points in restricted or controlled areas
* environmental and building architectural features used to gain access (trees, ledges, skylights, balconies, windows, tunnels)
* security screening devices (officer stations, surveillance, identification equipment)

References:

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 6.1.2 Controlled Access Zones;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-5.6.1 Site Evaluation, Grading, and Drainage

Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Chapter 6 “Understanding CPTED and Situational Crime Prevention”. CRC Press; Boca Raton, Florida. 2008.

NFPA 730 Guide for Premises Security. National Fire Protection Association. Chapter 5, Security Threat Assessment. Quincy, MA. 2006 Edition, 2010 update.

NFPA 101 Life Safety Code. National Fire Protection Association, Chapter 4 – General, Chapter 5 – Performance Based Operations, Chapter 18 – New Health Care Occupancies, Chapter 19 – Existing Health Care Occupancies, Chapter 20 – New Ambulatory Health Care Occupancies, and Chapter 21 – Existing Ambulatory Health Care Occupancies. Quincy, MA. 2009 Edition.

National Institute for Occupational Safety and Health, (NIOSH) Department of Health and Human Services. *Guidance to Protecting Building Environments from Airborne Chemical, Biological or Radiological Attacks*. Centers for Disease Control and Prevention. Cincinnati, OH. May 2002.

*Using building architecture to defeat access control systems:* [*http://www.youtube.com/watch?v=vfVKYa4a6qk*](http://www.youtube.com/watch?v=vfVKYa4a6qk)

Questions:

(Answer these questions below for each side in the Side Specific Description, in a descriptive, narrative form.)

* Are all access control elements (e.g. gates, guard booths, keypads, fencing, and barriers) in good repair and fully operable?
* Does the perimeter design allow access to the asset from any non-intended entrances?
* What type of vegetation exists on the asset perimeter, and are trees and other types of vegetation placed and maintained so that they cannot be used to gain access to the facility; or defeat a perimeter access control measure?

Side Specific Descriptions:

For each side (below) list and describe what elements are used to control this asset’s vehicle and pedestrian perimeter access? (e.g., fencing, walls, pivot and slide gates, security guard checkpoints, border vegetation, trespass signage, environmental barriers, etc).

Side A: South

Side B: West

Side C: North

Side D: East

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Options for Consideration – Perimeter Access Control

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# V. Proximity/Stand-Off

Guidance:

Standoff distance is a security measure that focuses on preventing unscreened vehicles and persons from approaching within a certain distance of a building. It is intended to deter vehicle, or hand carried bombs/weapons by making it more difficult for them to cause catastrophic damage. Many different measures can be used to provide standoff distance. Distance is the most effective and desirable tool because other measures vary in effectiveness, are more costly, and often have unintended consequences. Standoff measures must have the ability to defeat a moving vehicle whether it is using speed or maneuvering capability to reach its target.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-2.3; 2.4.1

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-4.4.7; 5.9.

Questions: (Answer/consider these questions below for each side in the Side Specific Description in a descriptive, narrative form.)

* Has it been determined how much stand-off distance is desired for this asset and its controlled access zones?
* Are vehicles and pedestrians “channelized” once they enter the asset campus?
* **Are physical barriers of sufficient strength to defeat any type of vehicle?**

Select the following applicable critical asset components located near any vehicle or pedestrian circulation areas? Could a vehicle drive through an entrance and penetrate the inner building space?

[ ] Emergency Generator(s);

[ ] Exposed Water Supply Infrastructure (Potable (Drinking) & Fire Suppression);

[ ] Exposed Wastewater Infrastructure (Lift Stations or Collection System Appurtenances)

[ ] Fuel Storage (above and below ground);

[ ] Fuel Supply (Natural Gas Meters)

[ ] Connection(s) to Commercial Power & Electrical Power Vault/Switchgear and Main Motor Controls

[ ] Telecommunications and IT Infrastructure;

[ ] HVAC Infrastructure;

[ ] Elevator Machinery and Control Rooms;

[ ] Bulk Liquid Oxygen and Hospital Medical Gas Tank Storage

Side Specific Descriptions:

For each side (below) consider the questions (above) and list/describe what elements are used to provide structural standoff protection (e.g., vehicle barriers, planters, walls, stairways) and the standoff distance they provide?

Side A: South

Side B: West

Side C: North

Side D: East

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Proximity/Standoff

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# VI. Lighting

Guidance:

The fundamental premise is that intruders do not wish to be observed. A basic level of lighting should allow the identification of a face from a distance of about 30-feet for a person with normal vision. Darkness and shadowing can provide areas of concealment where intruders or harmful devices can be hidden. Security lighting should be provided for the perimeter, campus interior, and building, and allow security personnel to maintain visual-assessment during darkness. The proper application of lighting can provide both a real and psychological deterrent for continuous or periodic observation.

Light fixtures should be protected against casual vandalism by means of tamper resistant materials location and design. Lighting should take into account vegetation, such as maturing trees, and other obstructions that would cause light to be blocked off. Lighting requires maintenance to preserve visibility. Bushes and trees that block off light should be trimmed to reduce shadow areas that can provide concealment. Lighting fixtures should be located at suitable heights for easy maintenance and replacement. Light fixtures should be maintained in a clean condition and promptly replaced if burnt or broken.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 2.9Physical Security Lighting;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-5.10 PHYSICAL SECURITYLIGHTING; 6.9 PHYSICAL SECURITY LIGHTING

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 3.3.4.2 Exterior-Mounted Electrical and Communications Equipment;

*Guideline for Security Lighting for People, Property and Public Spaces*, Illuminating Engineering Society of North America, 2003, New York, NY. (IESNA G-1-03 March 2003)

Unified Facilities Criteria (UFC) Design: Interior and Exterior Lighting and Control. U.S. Department of Defense.UFC 3-530-01 August 2006.

Questions: (Answer/consider these questions below for each side in the Side Specific Description, in a descriptive, narrative form.)

* Describe the lighting sources on campus (e.g., pole mounted, canopy, wall mounted, landscaping, etc.)
* How and when does the campus lighting activate (timer, photo-sensor, or manual; dusk to dawn, etc?)
* While observing during evening hours, does the existing lighting have obvious shadow areas? Identify any obvious show areas?
* Is campus lighting enhanced by adjacent facility or street lighting? If so, describe how/where?
* What areas are under emergency lighting? (zones covered by CCTV, high security areas, stairwells, exit markings, ingress/egress corridors, etc.)
* Is lighting on emergency power circuitry, and, does it have an automatic battery backup?
* Is lighting adequately provided such that a person can recognize a face from about 30 feet away?
* Are light fixtures protected against vandalism or made of vandal resistant materials?

Side Specific Descriptions:

For each side (below) consider the questions (above) and list/describe the types of lighting sources used on this campus? (e.g., pole mounted, wall mounted, canopy, landscaping, etc.)

Side A: South

Side B: West

Side C: North

Side D: East

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Lighting

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# VII. Signage

Guidance:

Signage should be used to assist in controlling authorized entry, deterring unauthorized entry, and to precluding accidental entry. Signs should be plainly displayed and legible from any approach to the perimeter, and from within the property boundaries, from a reasonable distance. Signs should be standardized to give clear, consistent, concise and readable messages that clearly identify areas of general accessibility and controlled entry.

For example, signage and graphics tell users about entrances and exits, direction of traffic flow, unauthorized areas, use of video surveillance, fire exits and alarms, panic buttons and intercoms for assistance, weapons policy, etc.

**1. SIGN DESIGN**

Signs should be large, legible and identifiable. The use of strong colors, standard symbols, simple shapes and graphics helps the reader understand the sign’s message.

**2 MESSAGE**

Signs should convey the message with adequate information. The message should be conveyed in suitable language(s) or pictographs.

**3. SIGN LOCATION**

Signs should be strategically located at entrances and near activity nodes (e.g., intersections of corridors or paths) and placed for visibility at an appropriate height.

**4. MAINTENANCE**

Signs should be maintained on a regular basis to ensure that they are visible. This may involve trimming any landscaping growth or cleaning the sign.

**5. MAPS**

In large campuses and buildings, maps containing information appropriate to the different needs of various groups of users should be available.

**6. HOURS OF OPERATION**

Where and when exits are closed should be indicated at the entrance of a route.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003 2.6 Signage;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007- 5.7 Signage; Florida Statutes 810.09 and 810.011

Questions: (Answer the questions below in a descriptive, narrative form.)

* Define how directional and no trespassing signage are posted. (e.g. perimeters and building entrances)
* How and where are hazardous material and weapons policy signs posted on campus?
* What asset signage (for highly sensitive areas, critical nodes or infrastructure) can be used by an attacker to identify and locate a possible target?
* Describe signage characteristics? (visible, legible, placement, clear message conveyance)
* How are signs, strategically located to allow for maximum visibility?

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Signage

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# VIII. Ingress/Egress

Guidance:

Building access control measures for healthcare facilities should include consideration to establishing a program to control access by personnel, vendors, and visitors. Identification cards should be issued to all employees, physicians, volunteers, students, and contract staff according to the hospital’s security vulnerability assessment. The cards should have as a minimum, a photograph of the bearer, at least the bearer’s first name, and the bearer’s position title.

Employees should be required to display their identification cards at all times. Visitors should not be able to access patient areas without passing the reception area. Facilities should consider the use of visitor logs or badges.

Access to uniforms, such as maintenance workers, and if possible, patients’ gowns, and doctors’ scrubs should be controlled. When intruders are able to obtain such garments, they are able to blending with health care staff.

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

To maintain proper emergency responder ingress/egress, routes and entrances leading to this asset should be designed to pro­vide the safest approach during an incident.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003

2.2.3 Vehicular and Pedestrian Circulation; 2.3 Standoff Distances; 2.4 Controlled Access Zones;

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 6.5.1 Emergency Egress Routes

Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Chapter 8 “Premise Liability”. CRC Press; Boca Raton, Florida. 2008.

Questions: (Answer the questions below in a descriptive, narrative form.)

* How are road ingresses/egresses access controlled?
* Define how the asset coordinates with local response agencies to determine primary and alternate ingress/egress routes for vehicle traffic?
* Who has primary responsibility to perform ID checks as persons enter the building?
* Describe how closets holding uniforms are controlled?

Options for Consideration – Ingress/Egress

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# IX. Parking

Guidance:

All parking should preferably be located outside the stand-off zone for all buildings and critical infrastructure. For the safety of staff and visitors, parking lots and garages should be properly illuminated, under CCTV surveillance, and provide emergency communication systems (e.g., intercom, telephones, etc.) to permit direct contact with security personnel.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003 2.2.3 Vehicular and Pedestrian Circulation; 2.7 Parking;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007- 5.8 Parking; 6.7 Parking.

Questions: (Answer the questions below in a descriptive, narrative form.)

* Describe the types of parking areas (lots and/or garages) and their designations on campus (e.g., general use, mixed use, employee, emergency room, etc.)
* What method(s) of access control are applied to parking areas?
* How many emergency intercoms or call boxes are used in the parking areas? Are they readily identifiable, well illuminated and under CCTV surveillance?
* Define the area(s) on campus which constitute drop off zones?
* If a valet service is used on campus, describe their access to the asset, parking areas, and operational hours?
* How are escorts used to transport/accompany staff to their vehicles at night?

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Parking

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# X. Surveillance

Guidance:

Seeing and being seen is critical to effective security. The more visible your location is from the street or ground level, the harder it is for an intruder to ingress, find concealment and escape unnoticed. You can implement natural surveillance in two ways: maintain clear “sight lines” around your property, and encourage positive social interaction. Building form, placement, and landscaping inherently define the “sight lines” within a space; and management of the threat of hostile surveillance is a consideration in the protection of people, property, and operations. Denying aggressors direct surveillance of a potential target, either from an external structural vantage point, on, or offsite, increases the ability to provide protection.

Providing opportunities for internal campus surveillance, both natural and technical, can be highly effective in discouraging and reducing malevolent activities. Proper surveillance means that people can see what others are doing, and people feel safe in public areas when they can easily see and interact with others. Would-be attackers are often deterred from committing acts in areas with high levels of surveillance. The fundamental premise is that intruders do not wish to be observed, and surveillance increases their perceived risk.

Increasing natural surveillance can be achieved by a number of techniques, including: landscaping, window treatments, lighting, the removal of obstructions, etc. Surveillance can be enhanced through active security patrolling combined with CCTV camera monitoring.

Perimeter and campus landscaping needs to be positioned/trimmed to ensure that foliage and thick trunks do not block important sight lines or create hiding places. In general, vegetation near the asset should be kept at a height and density that does not provide areas of concealment for people or objects; or isolated areas that are not easily observed. Keeping a clear site ‘window’ with ground vegetation lower that 2-3-feet and no branches lower that 8-feet to allow natural surveillance. Trees with trunks larger than 6-inches in diameter, poles (e.g., light fixture poles, flag poles, and power poles), or towers (e.g., electrical transmission and large communication towers) should not be placed too close to the asset.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 2.2.5 Landscape and Urban Design

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-5.13 Landscaping Plant selection and Design;

Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Chapter 10 “Terrorism and Infrastructure Protection: Risks and Protection”. CRC Press; Boca Raton, Florida. 2008.

Questions: (Answer the questions below in a descriptive, narrative form.)

* How is landscaping positioned and trimmed and does it serve as an obstruction to campus “site lines”?
* How is CCTV used on the campus? (*See* [*Video Surveillance Section*](#_XIV._Video_Surveillance))
* Identify any outside perimeter locations (street level or higher adjacent structure) that allow viewing of sensitive asset operations (e.g., hills, buildings, parking structures, other facilities, etc.)?
* How is asset security forces trained to recognize and react to hostile surveillance situations?
* How are "warning" signs placed on campus? (e.g., visible, no trespassing, security onsite, CCTV video surveillance in use, etc?). ([*See Signage Section*](#_VII._Signage))
* Describe any pedestrian and/or vehicle traffic which allow uninhibited access routes to perform mobile surveillance throughout the campus?
* Describe any procedures that exist to identify and verify disabled vehicles, personnel, etc. found in close proximity to the asset’s security perimeter or to internal critical components?
* What are the campus procedures visually recording vehicles and/or pedestrians who enter the campus?
* What are the campus procedures for reporting suspicious personnel or activities?
* Identify any campus lighting design that does not allow for clear sight lines and visibility? ([*See Lighting Section*](#_VI._Lighting))

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Surveillance (EXTERNAL)

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XI. Security Measures

Guidance:

Security measures include how the asset approaches safety/security issues for staff and visitors as well as the continuity of day-to-day operations. Security measures are only effective when they are communicated to the all employees, trained on, and exercised.

References:

U.S. GSA, Site Security Design Guide, Chapter 2 Guidelines for Elements and Innovations. Washington, DC: Government Printing Office, 2007. 11.

"Effective Site Security Design, Building Blocks for Effective Site Security." *Whole Building Design Guide*. National Institute of Building Science, 2009. Web. 1 Apr 2010. <http://www.wbdg.org/resources/effective_sitesecurity.php>

Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Chapter 11 “Problem Seeking before Problem Solving: Gauging Your Asset Base. CRC Press; Boca Raton, Florida. 2008.

Questions: (Answer the questions below in a descriptive, narrative form.)

* What types of onsite security force is present on this campus? (e.g., vendor, employee, local law enforcement, uniformed, armed/unarmed, level of training and licensure, shift variations, etc.)
* What type of communication is used by security personnel? (radio, cell phone, intercom, etc.)
* What is the asset’s standard patrolling procedure, and do they use verify the rounds with check points, badge swipes or other means? (foot patrol and/or vehicle)
* How are the asset security officers trained in coordinated response and lockdown procedures?
* Identify the designated security control room and/or console in place to monitor security cameras, fire alarm, and other asset security/safety systems?
* What security measures are found of the asset’s written plans? ([*See Plans & Procedures*](#_Plans_and_Procedures)*)*
* What type of contraband item search at pedestrian entrances does the asset conduct and do they make use of equipment such as Metal Detectors, Magnetometers or Hand Wands, etc.)
* How is asset security officers trained to confiscate and/or store weapons brought into the hospital?
* Define the asset security force’s direct relationship with local Law Enforcement and Fire Rescue organizations? (joint training, joint exercises)
* Describe how asset security measures include staff awareness programs and/or reporting policies for unusual activities?

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Security Measures

* Consider registering on the Florida Department of Law Enforcement’s “Business Safe” website at:<http://www.fdle.state.fl.us/Content/getdoc/fdebe58e-54e5-47a6-957d-f0d48de2b726/BusinesSafe-Home.aspx>

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XII. Personnel

Guidance:

A local or county search is critical because less than half of all states have criminal data repositories, and in some states only crimes less than seven years old are allowed to be reported for a background screening. Where available a statewide search should also be obtained. Since crimes are never limited to the places where applicants reside, but also occur when visiting or passing through a jurisdiction, a national search should also be conducted on the National Crime Information Center. This should also include the National Wants and Warrants system and Sexual Offender Databases to ensure the full spectrum of history is discovered. Another important look into an applicant’s history should include a Federal Search due to jurisdictional reporting. Crimes such as tax evasion, drug trafficking, and mail fraud, are under federal district court records.

Background screenings are like a snapshot in time. While the person in the photo stays the same, the reality is that people and life circumstances change. While a good rule of thumb is to re-screen during all transfers, and promotions, this is especially important as an employee’s job responsibilities increase. Many employers also use a five-year benchmark to re-screen their employees as a more uniform application of the re-screening process. Additionally, all contractors and vendors that are given access should be required to provide documented proof that the checks have been done.

References:

"Briefs." *Briefs Focus*. Hospital Association of Southern California, 04/2009. Web. 11 Mar 2010.

<http://www.hasc.org/download.cfm?ID=29531>

"Background Checks: Best-Practices for Financial Institutions. " *Bank Information Security Podcasts*. Web. 11 Mar 2010. <http://www.bankinfosecurity.com/podcasts.php?podcastID=89>

Questions: (Answer the questions below in a descriptive, narrative form.)

* To what level are potential applicant’s background screened? (local/county, state, national, federal)
* What type of re-screening procedure is practiced?
* What is the process for pre-determining the types and kinds of background history which are not compatible with employment in a healthcare environment, such as a grading system, or a pass/fail matrix?
* What types of NIMS compliant training has this asset offered to its personnel?
* .
* Who has attended the NIMS courses?
* .

Options for Consideration – Personnel

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XIII. Interior Access Control

Guidance***:***

Hospitals can to mitigate unauthorized access by incorporating visitor management systems, proximity card readers, a properly trained security response force, proper locks and key controls, and other physical barriers. In addition, all staff should be trained to recognize ID badges and challenge possible intruders. Interior (campus) critical areas such as HAZMAT storage, electrical, water, telecommunications infrastructure, and the helipad require adequate physical barriers to prevent unauthorized access and provide some protection in the event of an explosion or chemical release. Interior (building) access control should include considerations on how to have accountability for persons entering public and private spaces. Employees should be required to display their identification cards at all times. Vendors and service reps should be issued identification badges or temporary visitor badges that define what areas they are allowed in. Visitors should be issued temporary time sensitive identification badges and not be able to access patient areas without passing through a manned reception area.

Sensitive areas within a facility may warrant special protection access control with security technology, staffing, and restricted circulation. The level of protection may be based on zones of differing security levels. The idea is to allow employees, visitors, vendors, and others to reach their destinations and to prevent them from entering areas where they have no business. Controlling access to each department of a building, where appropriate, screens out undesirable visitors, reduces congestion, and helps employees identify and challenge unauthorized persons. Interior (building) access to areas such as: (emergency, labor & delivery, pediatrics, pharmacy, hotlab, etc.) should be strictly controlled with solid core doors, access cards, CCTV, and possibly biometric verification.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-2.3 STAND-OFF DISTANCE; 2.4.1 Physical Protective Barriers; 2.4.3 Anti-ram Vehicle Barriers; 2.5 ENTRY CONTROL AND VEHICULAR ACCESS;

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 6.1.3 Physical Protective Barriers;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-4.2.1 Issues of Barrier Systems Design; 4.4 PASSIVE BARRIERS; 4.5 ACTIVEBARRIERS; 5.3 ACCESSCONTROL POINTS; 6.5 Access Points;

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-2.3 Stand-off Distance; 2.4.1 Physical Protective Barriers;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-4.4.7 Fences

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-3.3.4 Doors; 3.9 ENTRY-CONTROL STATIONS

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-6.5 Access Points;

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 -3.3.3.1 Exterior Doors; 3.4.3.1 Exterior Doors; 3.6.2.1 Sectional and Rolling Doors

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007-4.3.3.1 Exterior Doors; 4.3.3.2 Exterior Doors in Hurricane-Prone Regions

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003;

3.3.5 Roof System Design

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 6.3.5.2 Roof System

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007

3.3.3.4 Roof Systems; 3.4.3.4 Roof Systems3.3.4 Nonstructural systems and equipment; 3.6.2.3 Roof Coverings;

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007; 4.3.3.7 Roof Systems; 4.3.3.8 Roof Systems in Hurricane-Prone Regions

Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Chapter 1 “What, Me Worry?”, Chapter 2 “Getting Started”, Chapter 6 “Understanding CPTED and Situational Crime Prevention”, Chapter 11 “Problem Seeking before Problem Solving”, Chapter 12 “Assessing Threats and Risks”, Chapter 14 “Protecting Building and Infrastructure with CPTED”. CRC Press; Boca Raton, Florida. 2008.

Questions: (Answer the questions below in a descriptive, narrative form.)

* What types of access control are being used on interior doors?
* .
* What are the different types of interior zones, or areas, which have controlled access?
* .
* Are ID badges also used for doorway access control?
* .
* Do procedures exist for activation/deactivation of access?
* What policy, procedure, and/or technologies does the facility have to lockdown the facility?
* .
* What is the visitor access policy and is there a system in place to provide temporary ID cards to visitors/outside contractors/vendors/janitorial personnel in the facility?
* .
* Is there a visitor log, which reflects date, time, name, company, and vehicle information?
* .
* Does the facility have a key-control policy? What person(s) outside of the agency has keys or codes to the facility?
* .
* Does the building have safes, or a safe room for valuables? If so, describe the location and security?
* .
* Where is the most actively used/high occupancy rooms in the hospital were the most number of casualties could be created?
* .
* How is access to the roof controlled, and can intruders access wall mounted ladders, or cross over from adjacent buildings?
* .
* Is there any underground access to the building?
* .
* What is the asset’s policy on “piggy backing” an access controlled door, and what training do staff members receive on this expectation?
* .

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Interior Access Control

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XIV. Alarms & Sensors

Guidance:

Electronic security, including door, window, and panic/duress alarms, and motion sensors are key elements of facility protection. All exterior doors, and windows up to scalable levels, should be alarmed, and motion sensors should be placed in all exterior rooms and hallways. Alarms should be constantly monitored by an onsite monitoring center on a 24-hour basis. A backup control center should be provided in a different location, such as a manager's or engineer's office, and when feasible, an off-site location should be considered. Automatic notification of local fire responders (fire and police) should also be considered.

Panic/duress alarms need to be in critical areas such as the front desk, newborn, pediatrics, emergency rooms, triage stations, reception, money handling areas, and other sensitive areas. Panic/duress devices can be in the form of a personal device, panel or desk button. Any alarm system should have battery backup to ensure that these systems can be maintained if the main electrical power goes down and the initiation of back up electrical power is delayed for some reason. Panic/duress alarm stations should be placed in clear view of CCTV cameras so that security can perform a video verification before deploying response.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-3.6 FIRE PROTECTION SYSTEMS; 3.8 ELECTRONIC SECURITY SYSTEMS

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003 6.5.8 Smoke and Fire Detection and Alarm System 6.5.9 Sprinkler/Standpipe System

Questions: (Answer the questions below in a descriptive, narrative form.)

(What types of alarms are in place at this facility?)

[ ] Burglar

[ ] Fire

[ ] Carbon Monoxide

[ ] Panic/Duress

[ ] Glass Breakage

[ ] CBRNE Detectors: Describe\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ] Audible

[ ] Motion

[ ] Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Which alarms are monitored onsite?
* .
* Who is the facility alarm monitoring company? (Phone number?)
* .
* How are the video, door alarms, intercom functionally integrated as a system?
* .

Options for Consideration – Alarms & Sensors

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XV. Video Surveillance

Guidance:

A video surveillance system servers as a force multiplier, by allowing a well trained security officer to monitor multiple locations from a single command center and alert others to an undesirable or dangerous situation. A well-installed system can be used in high traffic, limited access, increased threat, or ingress/egress areas to serve as deterrent and video evidence.

When properly installed the system should allow the operator to view the faces of person in the areas mentioned above, and reduce blind spots, where malevolent persons could avoid detection. When viewed from a video display, the system images should appear clear and free from haze. This is evidence that the cameras are properly focused, free from weather intrusion, and the lens and housing are clean.

Systems should be installed to record not just display imagery for future review, and stored for a locally agreed upon time frame, usually 30-days. In many cases it is also advisable that this data is stored offsite when possible to increase its survivability in the event of a disaster.

References:

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007.

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-3.8 ELECTRONIC SECURITY SYSTEMS.

*FBI CCTV Video Link* [*http://www.fbi.gov/news/stories/2010/march/cctv\_032310/caught-on-camera-best-practices-for-cctv-systems*](http://www.fbi.gov/news/stories/2010/march/cctv_032310/caught-on-camera-best-practices-for-cctv-systems)

Questions: (Answer/consider the questions below in a descriptive, narrative form.)

* Are critical assets (e.g. bulk liquid oxygen, fuel storage, utilities) as well as property ingress/egress, building entrances/exits, loading dock, and parking areas covered under external CCTV?
* .
* Describe the internal CCTV system. (include: camera types, placement, coverage area, monitored, recorded)
* .
* Are there gaps (“blind spots”) in the coverage of the internal CCTV system, and are they caused by factors such as: improper placement, vandalism, inadequate maintenance?
* .
* Are critical areas (e.g., newborn, pediatrics, emergency, radiology) as well as lobbies/common areas, hallways, stairwells, elevators, cafeteria, auditorium, etc. covered by internal CCTV?
* .
* Are camera housings and wiring secure and tamperproof?
* .
* Are cameras installed in overlapping patterns so that every camera is within the recorded view of another?
* .
* How long are images and video archived?
* .
* Define the asset’s monitoring capability. (e.g., number of camera monitored per-staff member, who conducts the surveillance, are they trained to recognize suspicious activities, is the system event driven, etc.)
* .

(Answer/consider these questions below for each side in the Side Specific Description in a descriptive, narrative form.)

* Describe the external CCTV system for each side of the facility? (include: camera types, placement, coverage area, monitored, recorded)
* Are there gaps in the coverage of the external CCTV system, and are they caused by factors such as: vegetation blockage, insufficient lighting, improper placement, vandalism, inadequate maintenance?

Side Specific Descriptions:

Side A: South

* .

Side B: West

* .

Side C: North

* .

Side D: East

* .

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Video Surveillance

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XVI. Communications

Guidance:

Having a well thought out strategy for redundant communication is the difference between being an isolated island and working well within the greater community. Asset managers must assume that when commercial hard-line networks fail that cellular technology will also be impacted. Using radio and satellite technology to bridge the gap on campus, to partner organizations and the government will help to ensure your facility is able to ask for help, and render aid when necessary.

Communication capabilities must be robust enough to withstand local natural disasters, or deployable in the event of one. They must be independently powered for at least 24-hours, and able to be re-charged. Communications strategies must also be compatible with other critical assets and local responders.

Intercoms can be integrated into hospital telephone systems or can be free-standing products. They should be able to make it possible to make announcements system wide as well as more selectively. Intercoms can be augmented with cameras and call buttons at entries. Wireless technology may offer some cost savings in installing new systems and existing WAN or LAN systems can provide a framework that new intercoms can tap into.

Public address systems can be a valuable addition for crisis management. These systems can be hardwired and installed at fixed locations or they can be portable. Public address systems can be plugged into conventional outlets or can run on rechargeable batteries. Newer technologies allow users to send messages to any text type device or the network, including displays, or customized for a broadcast across the health care campus.

Call boxes can be installed throughout the grounds of the facility and make it easy for building users to call for help. They may be made more useful by adding other features, such as speaker that tie into a public address system. Integration of CCTV then activates if the boxes are being used for prank calls or someone in distress.

Digital displays are especially helpful communication devices for lobbies and waiting rooms to communicate updates or important information. In addition to text messaging and email systems digital display devices are becoming commonplace in health care and emergency message distribution tools.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-3.7 COMMUNICATIONS SYSTEMS

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.5.11 Communication System

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 -4.4.10 Communications Systems

Questions: (Answer the questions below in a descriptive, narrative form.)

* What type of primary communication capabilities are utilized at this facility? [phone system types, analog/digital/fiber optic communication lines, pagers, radios, cellular phones]
* .
* What types of redundant communication are in place at this facility? [Med8, Satellite Phone…]
* .
* How often is the asset’s redundant communication tested?
* .
* What type of mass communication capabilities exist at this facility, are they on back-up power?
* .
* Identify any gaps in coverage?
* .

Options for Consideration – Communications

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XVII. Critical Nodes

Guidance

The Critical Nodes of an Asset are described as:

* A physical location, piece of equipment, technology or other item that if lost or destroyed, would greatly affect the Asset’s ability to function or carry out their mission.
* A Critical Node is also anything within the Asset that could be used as a weapon. (i.e., Chemicals)

Based on the above criteria, identify the Critical Nodes for the asset.

Questions: (Answer the questions below in a descriptive, narrative form.)

* Is access to the critical nodes limited to authorized personnel?
* .
* Do the asset personnel monitor vendors/contractors working on Critical Nodes?
* .
* Do access control systems keep a record of who has access to these spaces and when?
* .
* How are doors to the mechanical room secured and alarmed?
* .
* Who outside of the asset’s custodial department has access to your Critical Nodes?
* .
* How are critical node areas monitored by CCTV?
* .

|  |  |
| --- | --- |
| **Name:** | **Bulk Liquid Oxygen** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **On-Hand Supply:****(How long can onsite supply sustain operations?)** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Storage Tank Data Plate (if available) |  |  |

|  |  |
| --- | --- |
| **Name:** | **Electrical Power Infrastructure** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |
| --- | --- |
| **Name:** | **Water Infrastructure** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| **Name:** | **Wastewater/Sewage Infrastructure** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |
| --- | --- |
| **Name:** | **Fuels** |
| **Description:****(fuel type(s)/amount(s)** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **On-Hand Supply:****(How long can onsite supply sustain operations?)** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Storage Tank Data Plate (if available) |  |  |

|  |  |
| --- | --- |
| **Name:** | **Natural Gas - Propane** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |
| --- | --- |
| **Name:** | **Medical Gases [compressed oxygen, helium, nitrogen, carbon dioxide, etc…]** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **On-Hand Supply:****(How long can onsite supply sustain operations?)** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| **Name:** | **Telecommunications (Voice)** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |
| --- | --- |
| **Name:** | **Telecommunications (Data)** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

|  |  |
| --- | --- |
| **Name:** | **HVAC Chillers** |
| **Description:** |  |
| **Characteristic:****(Function)**  |  |
| **Location:** |  |
| **Redundancy:** |  |
| **Attraction:** |  |
| **Consequence of Loss:** |  |
| **Describe Access Control** |  |

Options for Consideration – Critical Nodes – Chillers

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XVIII. Utilities

Guidance:

Access to a water distribution system, wastewater collection system, electrical power infrastructure, communications vaults, or other utility connections and infrastructure is an inviting target to a malevolent individual who wishes to attack a facility. Disruptions from manmade and natural disasters can often be difficult to detect, pinpoint in the system, and causes costly and time consuming repairs. Attacks to utility infrastructure are crimes of opportunity and represent a significant portion of the simplest mitigations to a facility.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-3.5 ELECTRICAL SYSTEMS;

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.5 MECHANICAL AND ELECTRICAL SYSTEMS; 6.5.2 Emergency Power System; 6.5.4 Transformers;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007; 5.12 Infrastructure and Site Utilities

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 -3.4.5.1 Electrical Power; 4.3.9 Mechanical and Electrical Systems;

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007;4.3.5.1 Electrical Power

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007-2.3.5.3 Potable Water and Wastewater System;3.4.5.2 Water Service; 4.3.8 Utility Systems; 4.4.8 Utility Plumbing Systems;

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-2.10 SITE UTILITIES

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007-4.3.5.2 Water Service

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-2.10 Site Utilities;

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 -- 3.4.5.3 Sewer Service; 2.3.5.3 Potable Water and Wastewater System; 4.4.8 Utility Plumbing Systems

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007- 3.3.9 Potable Water and Wastewater Systems;4.3.5.3 Sewer Service.

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.5.3 Fuel storage

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007; 5.12 Infrastructure and Site Utilities

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 --2.3.5.4 Storage Tank Installations

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007; 3.3.10 Storage Tank Installations

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007- 2.4.6 UTILITY INSTALLATIONS

Questions: (Answer the questions below in a descriptive, narrative form.)

Which of the following can be maintained by emergency power?

[ ] Emergency Lighting

[ ] Fire alarm system

[ ] Generators

[ ] Fire pumps

[ ] Telephone switch

[ ] Security system

[ ] Mechanical control rooms

[ ] Building Automation System

[ ] Elevators (one per bank)

[ ] Sump pumps

[ ] Sewer ejector pumps

[ ] Smoke control systems

[ ] Stairwell Pressurization Fans (multi-story)

[ ] UPS serving technology/server rooms/Generators

[ ] HVAC for technology/server, and UPS rooms

Electrical Power

* How is power transmitted to the asset? (from a single or multiple substations; underground or pole transmission lines)
* .
* Where do the commercial power transmission line(s) enter the asset boundary?
* .
* How are commercial power transmission line(s) protected as they enter the asset boundary?
* Define how the asset’s main electrical switchgear/motor controls protected from unauthorized access?
* How is the main electrical shut-off protected from unauthorized access?
* How long can this asset remain operational with the loss of commercial power?
* If the asset suffered the loss of key electrical supply and distribution components (e.g. switchgear, motor controls, main transformers), how long would it take to repair/replace?
* Describe the power system’s automated load redistribution capabilities?
* How often is this element examined/checked for evidence of tampering?

Emergency Power

* List the location, size, and fuel type/capacity of all asset generators?
* Are generators on Automatic Transfer Switches (ATS) or switched manually?
* Is the existing emergency backup generation system capable of powering asset critical functions?
* Does the existing emergency backup generation system have cold-start capacities to activate large components after a shutdown due to a loss of commercial power?
* How often are generators tested (on/off, load, full load) (weekly, monthly)?
* What is the procedure for refueling and maintaining generators? (vendor, onsite, contracts)
* .
* What assurances are in place to ensure fuel, spare parts, and operators will be available during prolonged incidents?
* How often is this element examined/checked for evidence of tampering?

Natural Gas

* What is powered by natural gas at the asset?
* What redundancies are in place in the event of the loss of natural gas to the asset?
* How are exposed natural gas infrastructure and components protected by physical security controls?
* How often is this element examined/checked for evidence of tampering?

Fuels

* What types of liquid fuels are used/ stored at the asset, where are they stored, and in what quantities?
* Describe the storage method (underground/above ground tank)?
* What type of containment system is in place? (block wall, double walled tanks)
* What security procedures are in place for delivery and storage of liquid fuels?
* What assurances are in place to ensure that sufficient amounts of liquid fuels will be available during prolonged incidents?
* Identify fuels stored near buildings or other critical infrastructure components?
* How often is this element examined/checked for evidence of tampering?

Water

* What is the source of drinking water for this asset?
* What physical security controls are in place at exposed water appurtenances on the asset property? (back flow preventer/check valve, distribution pipes)
* What is the asset’s procedure for water outages? (contracts, storage containers, bottled water onsite)
* What assurances are in place to ensure that sufficient amounts of potable water will be available during prolonged incidents?
* How often is this element examined/checked for evidence of tampering?
* If, potable water is treated onsite, what means of containment is used for chorline gas storage and containment?

Wastewater

* Who does the asset rely on for wastewater services?
* What physical security controls are in place at exposed wastewater appurtenances on the asset property? (lift stations, collection system pipes)
* What alternate water source will be used to facilitate the flushing of toilets?
* What are the plans at this asset which address the loss of wastewater services for prolonged periods?
* How often is this element examined/checked for evidence of tampering?

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XIX. HVAC

Guidance:

Air intakes should be located high enough to insure that unintentional particles like vehicle exhaust are not introduced into the building. Likewise intakes should be tamper resistant so that articles cannot be thrown into their openings. Enclosures over intakes should be sloped to encourage water to drain away from the opening, and prevent water intrusion. Many building standards recommend placing intakes above the fourth floor to maximize fresh air intake, while not locating them on the roof.

HVAC systems to critical areas should be inaccessible to the public, especially if the ducting runs through the public areas of the building. It is also more secure to have a ducted air handling system, versus sharing hallways above drop ceilings for return air. Non-ducted systems provide greater opportunity for introducing contaminants.

During chemical, biological, and radiological situations, the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects. Smoke testing of the air supply to critical areas may be necessary. The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack.

References:

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.6.5 Zoning of HVAC Systems

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007; 5.11

Questions: (Answer the questions below in a descriptive, narrative form.)

* Identify any HVAC intakes for the building that are not higher than 12 feet from the ground?
* .
* What type of filter system is being used in the facility?
* .
* What filter maintenance schedule is the facility on?
* .
* Where are HVAC shutoffs located? (are these areas secured)
* .
* What isolated areas in the asset have localized HVAC controls?
* .
* Describe your policy/procedure for inspecting external intakes? (i.e. does security or maintenance personnel perform routine checks?)
* .

Options for Consideration – HVAC

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XX. HazMat

Guidance:

All areas of HAZMAT storage should be protected, secured and never left unattended to reduce vulnerability.  Critical assets and buildings which serve as a chemical/gas storage center should never be left unsecured.

Bulk liquid oxygen is generally not explosive when released. However when placed near an asphalt surface, oil storage or other area where this liquid could come into contact with a combustible, great care should be given to containment systems. Oxygen reacts very violently with combustibles, and should be avoided whenever possible.

References:

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007- 2.4.6

FEMA. "Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks." Risk Management Series. #427. 2003. Chapter 6.5 page 6-36

Questions: (Answer the questions below in a descriptive, narrative form.)

* How is an explosion at the asset’s bulk liquid fuel storage able to disrupt adjacent critical nodes?
* How would a catastrophic failure of the bulk liquid oxygen storage tank(s) disrupt adjacent critical nodes?
* Define the asset’s liquid fuel spill containment capability? [gasoline, diesel, aviation fuel]
* How are biological hazardous substances stored /secured on-site and how often are they removed?
* Is there a Nuclear Medicine or Nuclear Research Facility onsite at this asset? If so, how is bulk radiological/ nuclear material stored /secured?
* Other than daily delivered or calibration sources, does this asset store nuclear/radiological substances on-site?
* Are Tier II or 302 chemicals stored on site? How are these substances stored/secured/reported? If so, identify the asset HazMat Coordinator, including 24/7 contact information.
* Do bulk liquid oxygen tank(s) have a containment system for both safety and security?
* Identify the fire alarms and or leak detectors in the area?

|  |  |  |  |
| --- | --- | --- | --- |
| **Type**  | **Location** | **Size/ Max. Capacity** | **Observation (***describe access control***)** |
| **Bulk liquid oxygen****DOT 1073** |  |  |  |
| **Oxygen, Comp. Gas****DOT 1072**  |  |  |  |
| **Helium****DOT 1046**  |  |  |  |
| **Nitrogen****DOT 1066** |  |  |  |
| **Carbon Dioxide****DOT 1013** |  |  |  |
| **Nitrous Oxide****DOT 1070** |  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Options for Consideration – Hazmat

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XXI. Interdependencies

Guidance:

The interdependencies among critical system elements create vulnerabilities that are different, and potentially more damaging, than those found when considering individual dependencies. Interdependencies are often difficult to accurately identify and serve to amplify the consequences of a disruption. Therefore, these must be understood and then managed to minimize the impact of deliberate disruptions, human error, system complexity, or natural disasters on the surety of your critical systems.

Questions: (Answer the questions below in a descriptive, narrative form.)

* How would the loss of this asset affect the local/regional infrastructure, government, or consumers of the asset’s services?
* How would the loss of this asset affect the loss of your service area?

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XXII. Dependencies

Guidance:

Whether from a natural disaster or malevolent attack, a loss of a mission-critical, externally supplied services (e.g., commercial power, natural gas and fuel, water and wastewater, etc.) or onsite critical infrastructure including: Telecommunications, Information Technology and SCADA (Supervisory Control and Data Acquisition) systems, HVAC, etc. can cause a major disruption to the continued operation of your facility.

The underlying processes and physical components responsible for a single specific service supply delivery reveal many dependencies both technical and non-technical. Facility infrastructures are constituted of many components and connections that can fail, which can reduce/eliminate the service level and/or propagating damages (domino effect) to other infrastructures. In order to minimize the effects of these events on your facility’s mission, the development of service redundancies and solutions for the protection of such infrastructures needs to be considered. Ideally, these functions should have geographic dispersion, physical security protection, as well as, a recovery site or alternate work location. While some of these systems may be well secured and have dedicated/automatic redundancies, some critical functions still may not have a backup, and constitute what are called “Single Points of Failure.”

Questions: (Answer the questions below in a descriptive, narrative form.)

(What key infrastructure does this asset depend on to operate?)

[ ]  Water

[ ]  Wastewater/Sewer

[ ]  Fuel

[ ]  Electricity

[ ]  Natural Gas

[ ]  Telecommunications/Data

[ ]  Supply Chain [medical and other critical goods]

[ ]  Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Describe the net effect of the loss (whether by intentional or unintentional means) of any one or a combination of the above? (consider time/cost to repair/replace, safety, and economic impact)

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XXIII. Food Handling

Guidance:

All food storage and preparation areas of a facility should be protected, secured and never left unattended to reduce vulnerability. Facilities should be knowledgeable of the source of all food products they procure to help ensure they are not susceptible to intentional tampering.

References:

"Guidance for Industry." *Commonwealth of Kentucky, Department of Public Health*. Guidance for Industry, n.d. Web. 6 Apr 2010.

<http://nhs.ky.gov/nslsbp/CD_ROM/KY%20School%20Food%20Safety/Terrorism/bioguidance.doc>

Questions: (Answer the questions below in a descriptive, narrative form.)

* Have you considered the countries of origin of the source of the food stocks that are procured for your facility?
* .
* Are facility food storage and preparation areas access controlled to only cleared facility staff?
* .
* Who provides dietary/food service staff?
* .
* Does the asset have the ability to track food product usage in the event of a food born related illness?
* .

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XXIV. Delivery Procedures [Loading Dock & Mailroom]

Guidance:

Most deliveries to a building are either delivered to a loading dock, in the case of boxes, pallets, and larger items, and the mailroom. In many facilities these two entities are managed under a single leadership structure, and most often collocated or within feet of each other.

Where possible, these portions of a facility should be located away from each other, other critical nodes, and visitor/patient areas. This will ensure that malevolent activity and accidents are isolated, where possible.

Ideally vehicles which access the loading dock and other delivery points should be prevented from parking within 50-feet of critical equipment, utilities, distribution systems and important assets which is housed on, or just off these areas. Additionally, when these elements are collocated they should be protected and/or shielded from one another.

Proper protocols should be used for mail opening and handling that includes sorters wearing rubber gloves, and a emergency shutdown valve to stop the air handling system for that zone in case something is released from an envelope or package The goal is not to have a toxic release and have the AC system in place be used to distribute the contaminate throughout the building.

There should be a strict policy of no unauthorized vehicular or pedestrian traffic in the loading dock and mail area. The entire area should be monitored and recorded on CCTV. Access control features should be used to transition the service areas into the interior corridor network of the healthcare facility. The goal is to have a security layered transition from public to private spaces by service and worker personnel.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003; 2.8 Loading Docks and Service Access;

FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007-5.9 Loading Docks and Service; 6.8 Loading docks and service areas

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-5.6 CBR DETECTION

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.6.4 Lobbies, Loading Docks, and Mail Sorting Areas

Questions: (Answer the questions below in a descriptive, narrative form.)

* Are entrances and exits at loading docks and service entrances maintained at negative pressure relative to the rest of the building with a means to reduce infiltration and outdoor debris?
* **Where are the common ingress points for deliveries?**
* **Is the delivery ingress/loading dock attended while doors are unsecured?**
* What types of vehicles are required/authorized to load or unload at the loading dock? (vendors, supplies, contractors…)
* Describe vehicle and pedestrian access control (fencing, barriers, guards) for the loading dock area?
* .
* Describe the loading dock’s CCTV coverage and monitoring?
* .
* What types of devices are used to transition from the loading dock receiving area into the interior corridor system of the healthcare facility? (e.g. access control, CCTV…)
* .
* What types of alarms are used on the loading dock roll down gates or doors, and when are they used?
* .
* Identify any deliveries that are left on the loading dock by couriers?
* .
* Where is mail received, sorted, and processed?
* .
* How are mail bins/boxes secured, to prevent unauthorized person from intercepting official communication?
* .
* What type of training do mail handling personnel receive to recognize suspicious packages?
* .
* How is the mailroom’s ventilation system isolated in the event of a toxic substance release? (localized HVAC system with an individual shutoff, panic button, sensors)
* .
* What type of filter system is used is the mail area HVAC zone? (e.g. pleated, HEPA…)
* .
* When is the dumpster area permitted to remain unlocked? (e.g. at all times, except when being used by authorized staff, business house)
* .
* Describe the dumpster area’s video surveillance coverage.
* .

Options for Consideration – Delivery Procedures (Loading Dock and Mailroom)

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XXV. Other Consideration

## Elevators

Guidance:

Elevators mechanical located in areas subject to flooding, elevator component equipment and controls will be damaged, and communication between floors will be impaired. Mechanical equipment or elevator machine rooms in elevator penthouses that do not adequately address protection of equipment on the roof. Public Elevators should limit the floors that are accessible to the public, and be able to be remotely monitored and stopped during a facility lockdown.

References:

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.5.7 Emergency Elevators

FEMA 543 Risk Management Series for Improving Critical Facility Safety from Flooding and High Winds, January 2007-3.4.4.1 Elevators

Questions: (Answer the questions below in a descriptive, narrative form.)

* How many banks of elevators does this building have?
* Who is the elevator maintenance provider? (name and 24/7 phone#)
* Where are the mechanical rooms located? (e.g., ground floor or roof penthouse)
* Identify the number of elevators in each bank on the back-up electrical power system?
* What type of CCTV coverage is used in the elevators?

## Windows

Guidance:

Windows are typically the most vulnerable portion of any building, especially in hurricane prone areas and coastal property. Though it may be impractical to design all the windows to resist a large scale explosive attack, it is desirable to limit the amount of hazardous glass breakage to reduce the injuries. Typical annealed glass windows break at low pressure and impulse levels and the shards created by broken windows are responsible for many of the injuries. To make sure that the components supporting the glass are stronger than the glass itself, specify a window breakage strength that is high compared to what is used in conventional design.

Windows should to be secured to prevent entry and unauthorized surveillance.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003 3.3.3 Window Design;

FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003-6.4.2 Window Design; 6.4.2.1 Glass Design; 6.4.2.3 Frame and Anchorage Design;

FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007 -3.3.3.2 Windows and Skylights; 3.4.3.2 Windows and Skylights; 3.6.2.2 Windows and Skylights;

FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007; 4.4.2.2 Windows and Skylights

Questions: (Answer/consider these questions below for each side in the Side Specific Description in a descriptive, narrative form.)

* Are windows on the ground floor, operable?
* Are the windows treated with a tint or damage resistant film? [wind/impact rating]
* What type of window treatment has been applied to this asset windows? [impact resistant, break reduction]
* Does window tint prevent visual surveillance into the building and enhance surveillance out the building at night.
* Is there glass breakage sensors placed in rooms with exterior windows?

Side Specific Descriptions: [include barriers which are used for access control]

Side A: South

Side B: North

Side C: North

Side D: East

## Pharmacy:

Guidance:

Pharmacies are used to store and distribute legend pharmaceuticals and present a special target within a healthcare facility. Pharmacy areas should be access controlled by a separate key with the pharmacist having direct control of the keys and or codes. Walls should be fire code to the deck all the way around the pharmacy. Any exterior windows should be non-operational and secured with glass break alarms and/or bars. Use of CCTV in the pharmacy serves as a deterrent to malevolent activity, thefts, etc. CCTV is also a useful tool for identification of persons requesting access to this secure area, and person loitering outside pharmacy ingress/egress doors.

References:

Physical Security Design Manual for Critical Facility, Department of Veterans Affairs, July 2007- 5.11 Pharmacy;

Questions: (Answer the questions below in a descriptive, narrative form.)

* Describe the main pharmacy? (location, firewalls, outer hallway, ingress/egress, in-house, commercial, hours, staffing plan)
* What type of access control is in place at the pharmacy? (e.g. keys, card reader, biometric reader)
* Are deliveries of medications monitored from the receiving dock to the pharmacy, or delivered directly to the pharmacy?
* Describe the physical security features in the vicinity of the dispensing point for medications?
* What type of doors alarms are in use?
* Is there a panic/duress alarm at the dispensing window or counter?
* Describe the CCTV coverage within and in the immediate vicinity outside the pharmacy. Can the CCTV outside the pharmacy be viewed by the pharmacy staff?

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Options for Consideration – Pharmacy

## Plans and Procedures

Guidance:

A plan is a documented "concept of operation" that describes the essential elements of advance planning that have been considered and the provisions that have been made to mitigate emergency situations. The plan should incorporate information about the emergency response roles of supporting organizations and agencies, and should be consistent with a graded approach to managing “all-hazard” incidents.

Procedures must be consistent and compatible with the plan, whether utilized in, or associated with, facility emergency response activities. Procedures must contain the detailed information and the specific instructions needed to carry out the emergency plan during a drill, exercise, or actual incident.

Well written plan are only effective when they are communicated to the all employees, trained on, and exercises. These plans should not exist in binders only; rather the facility should reproduce the actionable items in their plans and make task aids for easy use. This reduces confusion and increases the employee’s likelihood of success.

Consider written policies for hostage, terrorist, cyber attacks, mail handling and bomb threats. Bomb threat questions need to be located near phones for personnel to use to obtain as much information as possible about a bomb threat that is called into the hospital. Employees need to be trained to recognize and respond to suspicious packages. Policies should also be part of the training and exercise conducted at least annually.

References:

FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003- 5.1-2

Questions: (Answer the questions below in a descriptive, narrative form.)

* What does this facility call its emergency plans and procedures? (e.g., SOP, Hospital Plan, Emergency Procedures…)
* How often is the facility emergency plan exercised, and do other agencies participate?
* Does the facility have a written:

[ ]  Security Plan

[ ]  Hostage Plan **(Code White)**

[ ]  Terrorist Incident Plan

[ ]  Natural Disaster Plan **(Code Brown)**

[ ]  Mass Casualty Plan **(Code Green)**

[ ]  WMD Plan **(Code Orange / Code Yellow)**

[ ]  Emergency Evacuation and Shelter Plan (**Code Red/ Code Brown)**

[ ]  Continuity of Operations Plan

* What kinds of training (in emergency contingency plans, policies, and procedures) do employees receive? (when is the initial training provided, and how often is follow up training provided)
* Describe the training administrative personnel are provided in telephoned bomb threat procedures?
* .
* What is the policy and procedure to secure the ER in the event of a WMD attack?
* What is the emergency decontamination plan for the facility, patients, staff, outside mass casualties seeking assistance?

Options for Consideration – Plans and Procedures

## Fire Suppression

Guidance:

Fire protection involves detection and suppression of [fire](http://en.wikipedia.org/wiki/Fire) and its related emergencies. Owners and operators of structures are responsible to maintain their facilities in accordance with the local [building code](http://en.wikipedia.org/wiki/Building_code) and fire code, which are enforced by the [Authority Having Jurisdiction](http://en.wikipedia.org/wiki/Authority_Having_Jurisdiction) (AHJ). During construction, builders must comply with the version of the building codes that is in effect at the time of construction. After construction, buildings must be maintained according to the current fire code. In the event of fire emergencies, installed fire suppression systems (sprinklers, gas, and chemical), firefighters and occupants of the building (or any combination) may be called upon to suppress the fire and mitigate its spread to unaffected areas, or buildings.

Fire suppression refers only to [active](http://en.wikipedia.org/wiki/Active_fire_protection) (sprinklers, extinguishers and agents) and [passive](http://en.wikipedia.org/wiki/Passive_fire_protection) (fire stops) fire protection systems, and does usually not encompass [fire detection](http://en.wikipedia.org/w/index.php?title=Fire_detection&action=edit&redlink=1) systems such as [fire alarms](http://en.wikipedia.org/wiki/Fire_alarm) or [smoke detection](http://en.wikipedia.org/wiki/Smoke_detection). Alarms and detection are addressed in [Section XIII Alarms and Sensors.](#_XIII._Alarms_&)

References:

NFPA 1 Fire Code, National Fire Protection Association, Part I – Administration, Chapters 3 – 6; Part II – General, Chapters 10 – 14; Part II – General, Chapters 16, 18 and 19; Part III – Occupancy, Chapters 20, 26, 29, 34; Part IV – Processes, Chapters 41, 42; Part V – Equipment Chapter 50, 51 53; Part VI – Hazardous Materials, Chapters 60, 61, 63, 66, 69, 70, 71; Annexes A, B, D, K, O, P, R. Quincy, MA. 2009 Edition,

NFPA 10 Standard for Portable Fire Extinguishers, National Fire Protection Association Chapter 4, 5, 7; Annexes A, B, C, D, E, G, H. Quincy, MA. 2010 Edition

NFPA 13, Standard for the Installation of Sprinkler Systems, National Fire Protection Association, Chapter 4 – General Requirements. Quincy, MA. 2010 Edition

NFPA 14 Standard for the Installation of Standpipes and Hose Systems, Chapters 3 to 7, Fire Protection Association. Quincy, MA. 2009 Edition

NFPA 101 Life Safety Code. National Fire Protection Association, Chapter 4 - General, Chapter 5 – Performance Based Options, Chapter 18 – New Health Care Occupancies, Chapter 19 – Existing Health Care Occupancies; Chapter 20 – New Ambulatory Health Care Occupancies; and Chapter 21 – Existing Ambulatory Health Care Occupancies. Quincy, MA. 2009 Edition.

NFPA 291, Recommended Practice for Fire Flow Testing and Marking of Hydrants, National Fire Protection Association. Quincy, MA. 2010 Edition

Questions: (Answer the questions below in a descriptive, narrative form.)

* What type of standpipe system is in place at the facility? (wet, dry, automatic, manual, combined, etc.)
* Are the standpipes locked or chained to make them tamper resistant?
* Does the facility have hydrants on the campus and close to the facility?
* Is there hydrant flushing program in place at this facility? Who conducts the hydrant flushing program?
* What is the distance from the facility to the nearest fire station?
* For multi-story facilities and campus facilities, what is the distance to the nearest fire station with an aerial apparatus assigned?
* Is the building under 100% sprinkler coverage?
* Who is the vendor providing fire suppression systems (or equipment), alarms and other life safety equipment (i.e., respirators) provided under contract with this facility?
* Is there a chemical fire retardant (suppression) system used in server rooms or other sensitive areas (food service)?
* Who is responsible for the fire extinguisher inspection program at the facility?
* Are personnel trained to properly employ a fire extinguisher?

## Non-Agency Tenants

Questions: (Answer the questions below in a descriptive, narrative form.)

* Please identify any non-agency tenants of the building, to include their occupancy, emergency contact, location in the building?

## Special Events

Questions: (Answer the questions below in a descriptive, narrative form.)

* Please identify any special events that are held in the facility or on the campus grounds, including: event name, date, and number of attendees? Describe any security and parking modifications?

## Helipad

Questions: (Answer the questions below in a descriptive, narrative form.)

* Is there a helipad on the property?
* .
* If there is an elevated helipad, what is the maximum weight capacity, and can vehicles park adjacent to the helipad?
* .
* What type(s) of fencing or other physical barriers are used to secure the helipad?
* .
* Does CCTV coverage monitor the helipad?
* .
* Is the helipad illuminated for night operations?
* .

## Newborn/Pediatrics

Questions: (Answer the questions below in a descriptive, narrative form.)

* Is there a dedicated nurse’s station to challenge unauthorized persons?
* Describe the infant tagging system? Does it trigger a floor/elevator/stairwell lockdown?
* Describe the access control to the newborn and pediatric wards?
* Is video surveillance employed in the newborn and pediatric wards? If so, are cameras actively monitored and recorded?
* Does the facility have an active “Code Pink” or related testing process to ensure infant security is functional? If so, briefly describe the process?

Section Assessment Team

**Primary Assessor**: (Third Party or Facility Lead Representative)

**Asset/Unit Assessors**: (other local representatives, and/or facility personnel)

# XXVI. References

*Crime Prevention Through Environmental Design, Timothy D. Crowe*

*FEMA 426 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003*

*FEMA 427 Risk Management Series Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks December 2003*

*FEMA 430 Risk Management Series Site and Urban Design for Security Guidance Against Potential Terrorist Attack December 2007*

*FEMA 452 Risk Management Series A How to Guide to Mitigate Potential Terrorist Attacks Against Buildings*

*FEMA 543 Risk Management Series For Improving Critical Facility Safety from Flooding and High Winds, January 2007*

*FEMA 577 Risk Management Series Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds June 2007*

*Occupational Hazards in Hospitals DHHS (NIOSH) Publication No. 2002–101 April 2002“Designing Safer Communities,” National Crime Prevention Council, Washington DC;*

*Physical Security Design Manual for VA Facilities: Mission Critical Facility, Department of Veterans Affairs, Washington, DC 20420, July 2007*

*Florida Statutes 810.09 and 810.011*

*Department of Defense Minimum Antiterrorism Standards for UFC 4-010-01.8 October 2003,Including change 1, 22 January 2007*

*NFPA I, Uniform Fire Code, Florida 14.5.3.*

*Atlas, Randall. 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention. CRC Press; Boca Raton, Florida. 2008.*

*NFPA 730 Guide for Premises Security. National Fire Protection Association. Quincy, MA. 2006 Edition, 2010 update.*

*NFPA 101 Life Safety Code. National Fire Protection Association. Quincy, MA. 2000 Edition.*

*National Institute for Occupational Safety and Health, (NIOSH) Department of Health and Human Services. Guidance to Protecting Building Environments from Airborne Chemical, Biological or Radiological Attacks. Centers for Disease Control and Prevention. Cincinnati, OH. May 2002.*

*Guideline for Security Lighting for People, Property and Public Spaces, Illuminating Engineering Society of North America, 2003, New York, NY. (IESNA G-1-03 March 2003)*

*Unified Facilities Criteria (UFC) Design: Interior and Exterior Lighting and Control. U.S. Department of Defense. UFC 3-530-01 August 2006.*

*Florida Department of Law Enforcement’s “Business Safe” website:*

[*http://www.fdle.state.fl.us/Content/getdoc/fdebe58e-54e5-47a6-957d-f0d48de2b726/BusinesSafe-Home.aspx*](http://www.fdle.state.fl.us/Content/getdoc/fdebe58e-54e5-47a6-957d-f0d48de2b726/BusinesSafe-Home.aspx)

*Using building architecture to defeat access control systems:* [*http://www.youtube.com/watch?v=vfVKYa4a6qk*](http://www.youtube.com/watch?v=vfVKYa4a6qk)

*FBI CCTV Video Link* [*http://www.fbi.gov/news/stories/2010/march/cctv\_032310/caught-on-camera-best-practices-for-cctv-systems*](http://www.fbi.gov/news/stories/2010/march/cctv_032310/caught-on-camera-best-practices-for-cctv-systems)

# XXVII. Glossary of Terms & Acronyms

|  |  |
| --- | --- |
| * **CPTED**
	+ Crime Prevention Through Environmental Design
* **Natural Surveillance**
	+ In this report Natural Surveillance means, the ability of a person to look out across the campus unaided by cameras or other technology. The majority of the time the term is used when describing how landscaping and other obstacles (e.g., terrain features, outbuildings, parking garages, etc.) may visually obstruct an open area.
* **Access Control**
	+ A device, design, or system which enables an authority to control entry into a given physical space.
* **Intrusion Detection**
* Electronic security features that include: CCTV cameras, motion detection, door/window alarms, etc.
* **Territorial Reinforcement**
	+ Design and use of sidewalks, landscaping, fences and other physical elements to create a border (not always physically secured) between private and public property.
* **Commendable Action**
	+ This section of the assessment is used to highlight areas where the facility has overcome past challenges, implements creative problem solving, or developed a best practice.
* **Flood Zone Designation**
	+ This is the flood zone and/or coast storm surge designation given to an area where the asset is located.
* **Asset**
	+ This term is used interchangeably with facility, hospital, and location.
* **Critical Node**
* A physical location, piece of equipment, technology or other item that if lost or destroyed, would greatly affect the Asset’s ability to function or carry out their mission.
* **NFPA**
	+ National Fire Protection Association
* **FEMA**
	+ Federal Emergency Management Agency
* **Standoff**
	+ A certain distance between objects, usually the distance from a hazardous object.
* **Channelization**
	+ This is a design concept which used barriers, walkway layouts, vehicle traffic patterns, and signage to force pedestrian and vehicular traffic to travel in a certain direction or to a specified point; and away from unauthorized areas.
* **HVAC**
	+ Heating, Ventilation, and Air-Conditioning
* **Bollard**
	+ This is a post usually installed as a system or group which creates distance between where the posts are installed and either a sensitive piece of equipment or a building entrance. They can be permanent, removable or hydraulic (pop up).
* **CCTV**
	+ Closed Circuit Television
* **ATS**
	+ Automatic Transfer Switch: This equipment senses a loss of commercial power and send a signal to the emergency power system to activate.
* **Ingress**
	+ To enter a space or building.
* **Egress**
	+ To exit a space of building.
* **Call Box**
	+ This is usually a standalone pole, normally blue, that has either a phone or radio that can be activated to call for help in areas that may not always be patrolled. Call boxes are used on large campuses, and in parking garages. Many of these units also have a flashing light on top of them that helps identify where a person needs assistance as well as a camera that allows security personnel to see the person activating the unit.
* **EtO**
	+ Ethylene Oxide: This chemical is highly carcinogenic, but is very effective in uses for sterile processing.
* **UPS**
	+ Uninterrupted Power Source
* **Bulk Liquid Oxygen**
	+ Though oxygen is used at hospitals in gaseous form, storing it in liquid form tanks up much less space. When stored in liquid form, oxygen is at a cryogenic state, which means it can kill human tissue rapidly.
* **Penthouse**
	+ Used in this document, Penthouse refers to a space or room on the facility’s roof where elevator and other mechanical equipment are housed.
* **NIPP** (National Infrastructure Protection Plan)
* The National Infrastructure Protection Plan provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's [critical infrastructure and key resources (CIKR)](http://www.dhs.gov/files/programs/gc_1189168948944.shtm) into a single national program. <http://www.dhs.gov/files/programs/editorial_0827.shtm>
* **CI/KR (Critical Infrastructure/Key Resources)**
* Critical Infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.
* Key Resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.
* [Homeland Security Presidential Directive 7 (HSPD-7)](http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm)
* Established U.S. policy for enhancing CIKR protection by establishing a framework for NIPP partners to identify, prioritize, and protect the nation's CIKR from terrorist attacks. The directive identified 17 CIKR sectors and designated a federal Sector-Specific Agency (SSA) to lead CIKR protection efforts in each. The directive allows for the Department of Homeland Security to identify gaps in existing CIKR sectors and establish new sectors to fill these gaps. Under this authority, the Department established an 18th sector, the Critical Manufacturing Sector, in March 2008.
 |  |

# Appendix A – Instructions for Assessors

Title Page

Place the Full Legal name of the facility in the “Facility Name” place holder. Locally known names, and other common nomenclature for the facility may be placed under the legal name.

You will need to obtain an aerial photograph of the facility. Google Maps is an excellent source for these images when a facility does not have aerial photo to provide. To use the photo place holder, select the picture icon in the center of the place holder. In the window that opens select your aerial photo and click on ok. The photo should have loaded onto the page.

Visit the webpage [www.acha.myflorida.com](http://www.acha.myflorida.com) to look-up a facility’s licensed trauma rating and bed count. Record this information in the space provided.

Double click on the footer to enable editing of this content. Place the facility’s legal name in the header and foot sections, where indicated. Also update the indicated date field with the date of the onsite assessment.

Table of Contents

Any time changes are made to the document, the assessor should right-click on the table of contents and select “Update Field”. Choose to update only the page numbers where the section headings haven’t been adjusted, or select update entire field to capture substantive edits.

*With the use of this automatic table of contents, and the various hyperlinks in the document, please ensure that the use of styles like Header 1, or Header 2 are used only when you want the text to appear in the table of content.*

[Facility Profile](#_I._Facility_Profile)

This information is mostly available from publicly available sources on the internet. Start your interview of the facility staff with page to ensure all information is captured.

Some hospitals are multi-building campuses, where other supporting services, like labs, doctor’s offices, hospital administration, and esc... are collocated with the main hospital building to better serve the patients. When conducting an assessment of just the hospital, be sure to capture the total number of buildings on campus in the indicated field, even thought this assessment may not cover all buildings.

[Community Profile](#_Community_Profile)

The community profile tells the story of what surrounds this facility.

When a responder agency arrives on scene, there is often not enough time to orient their location and the location of the building with the cardinal directions. To aid in communication, and reduce confusion, responders immediately locate the main entrance and label that Side A. From Side A, the responder continues in a clock-wise direction and continues to label the sides B-D. In order to complete the Community Profile use the picture place holder to again place the aerial photograph in the report. Arrange the side labels as appropriate.

During your visit, on Google Earth take note of the cardinal directions so that they can be captured in the side specific description area, where indicated.

When answering the question, “*What bodies of water, airports, railroads, streets, major freeway access are near to the facility?*” consider that the word near is subjective. Some hospitals are built on major rivers or bodies of water and certainly “near” would apply here, but so would the railroad who operates three miles away and is known to transport hazardous materials. Should a train derail three miles away from an asset with HazMat on board, the hospital would most likely be affected. Near is subjective based on the area and the distance of surrounding infrastructure.

Example:

Side D

Side C

Side B

Side A

Side B

Notice in this example of the Lincoln Memorial, that the photo is oriented north. This is a best practice when using aerial photography. The main entrance is located to the east in this photo and is always labeled Side A, and the labeling format, follows a clockwise direction.

(note: compass direction in upper right corner of image)

Section Lay Out

Most sections of this report are designed to give the assessor, and reader, three pieces of key information. The “Guidance” portion is directive information that establishes a base line of best practices, industry standards, and required benchmarks where they were available. These tools are then used by the assessor to judge the asset by.

Sections may also have a “References” section that gives the assessor and reader additional resources, and the sources of the guidance standards.

Each section of this assessment also has a questions portion. This part of the report contains the detailed assessment information. This section may be presented in tables, narrative, or list format. Each narrative question should be answered in complete thought, not in a yes/no form.

Finally, each report, based on the assessor’s findings may have “Options for Consideration”. This portion of the report is where the assessor will indicate how to mitigate any areas of the report where the asset did not specifically meet the guidance criteria.

# Appendix B – Options for Consideration Summary

1. Recognizability – Use the “Insert Endnote” button in the “Footnotes” section of the “References” menu tab (Word 2007-2010) to sequentially number this option for consideration. [↑](#endnote-ref-1)
2. Recognizability – Use the copy or keyboard shortcut Ctrl+C to copy you option to reduce duplicative data entry. [↑](#endnote-ref-2)
3. Recognizability – If bullet formatting carries over to the footnote page, use the “Show/Hide” tool to insure that you are selecting only the text and punctuation marks of the option. Any paragraph symbols in your copy selection will for bullet formatting in the footnote. [↑](#endnote-ref-3)
4. Recognizability – Double click on the Endnote citation number in the document or on the Options for Consideration Summary page to toggle between the pages. [↑](#endnote-ref-4)