



# Security Guidelines for American Enterprises Abroad



by  
Alan Pruitt CPP



**This Page Intentionally Left Blank**





## Certified Security Information e-Books

Creative Commons (cc) Copyright 2007, Alan Pruitt CPP

Webcognita

[www.webcognita.com](http://www.webcognita.com)

Some rights reserved. Creative Commons Attribution – Non-Commercial – Share Alike 3.0

You are free **to share** – to copy, distribute and transmit this work. You are free **to remix** – to adapt this work...under the following conditions: **Attribution**. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work). **Noncommercial**. You may not use this work for commercial purposes. **Share Alike**. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one. Any of the above conditions can be waived if you get permission from the copyright holder (Webcognita). Nothing in this license impairs or restricts the author's moral rights.





**This e-Book is dedicated to the Professional Problem Solver that exists in all of us.**





**Disclaimer**

Alan Pruitt CPP has done his best to give you useful and accurate information, but it's your responsibility to verify all information discussed in this e-Book before relying on it. He doesn't guarantee that the information will be appropriate to your particular situation or even accurate. Laws, procedures and regulation change frequently and are subject to different interpretations. Every state has its own laws as well. Please obtain competent legal or technical advice from the appropriate government agency or legal advisor, before making your own decision.

Alan Pruitt CPP makes no representation or a warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or guaranteed success. Under no circumstance will he be held responsible for economic or non-economic damages resulting from the use or misuse of any furnished documentation or source. Further, he reserves the right to revise this publication and to make changes from time to time in the content hereof, without notice.

For years the world has recognized a need for competent professionals who can effectively manage complex security issues that threaten people and the assets of corporations, governments, and public and private institutions. As the emphasis on protecting people, property, and information increases, it has strengthened the demand for professional managers. To meet these needs, the ASIS International administers the Certified Protection Professional program. Nearly 10,000 professionals have earned the designation of CPP™. This group of professionals has demonstrated its competency in the areas of security solutions and best-business practices through an intensive qualification and testing program. As a result, these men and women have been awarded the coveted designation of CPP™, and are recognized as proven leaders in their profession. Alan was awarded the CPP™ designation in February 2003.



## TABLE OF CONTENTS

Forward .....	7
Chapter I. Introduction .....	8
Chapter II. Site Selection Guidelines .....	10
Chapter III. Exterior Protection.....	15
Chapter IV. Interior Protection .....	25
Chapter V. Public Access Controls (PAC) .....	31
Chapter VI. Emergency Exit.....	34
Chapter VII. Communications .....	35
Chapter VIII. Office Security Guidelines .....	37
Chapter IX. Vehicular and Travel Security.....	41
Chapter X. Visiting Personnel Protection.....	45
Appendix I. Security Survey Checklist.....	53
Appendix II. Facility Questionnaire .....	66
Appendix III. Threatening Phone Call Checklist .....	69
Appendix IV. Letter and Parcel Bomb Recognition Points .....	73



## Forward

**E**ffective security precautions require a continuous and conscious awareness of your environment. This is especially true when living in a foreign country where it will be necessary to adapt to new cultures, customs, and laws which, in most instances, are very different from those to which Americans are accustomed in the United States.

The implementation of security guidelines contained in this e-Book could reduce the vulnerability of American private sector enterprises abroad to criminal or terrorist acts. It is recognized that some of the recommended guidelines cannot easily be implemented at existing facilities.

This Webcognita e-Book is *re-purposed* from the original U.S. Department of State Overseas Advisory Council (OSAC) on-line document with the same title. This re-formatted version of the same document is intended to ease readability and encourage use of the information by interested readers.



## Chapter I. Introduction

This e-Book is a compilation of security guidelines for American private sector executives operating outside the United States. This guidance is the product of many years of experience by a cross section of American security practitioners from both the public and private sectors. Obviously, the implementation should be consistent with the level of risk in the country where you conduct business. For the most part the guidelines are for protection in high threat areas. It is recognized that the level of risk varies from country to country and time to time so that you may need to choose among the suggested options or apply the concepts in a manner modified to meet your needs. Since levels of risk can change very rapidly, it is advisable to continuously monitor factors that may impact the risk level. Security precautions must be flexible and dynamic to respond effectively to changing risks. A static, inflexible security posture will almost certainly result in a lack of preparedness or unnecessary expense.

The Department of State has three threat assessment designators: High, Medium, and Low. One of these three threat designators is applied to each country where the United States has diplomatic representation. Threat assessment information is available to the American business community in countries where the United States has diplomatic representation through the Regional Security Officer or Post Security Officer at the nearest U.S. diplomatic post, i.e. Embassy or Consulate. The level assigned to a particular country is determined by an analysis of the political, terrorist, and criminal environment of that country. It is reviewed quarterly by the Department of State and changed when appropriate.

A High Threat country is one where the threat is serious and forced entries and assaults on residents are common, or where an active terrorist threat exists. A Medium Threat country is one where the threat is moderate, with some forced entries and assaults on residents occurring, or where the area has the potential for terrorist activity. A Low Threat country is one where the threat is minimal and forced entry of residences and assault of occupants is not common, and there is no known terrorist threat.

For emphasis again, the guidelines set forth in this publication are generally most appropriate for High Threat areas. One will probably want to moderate them for applications where the risk is lower; or where other considerations preclude their implementation at the level discussed here. In many situations, professional technical security assistance will be required.



These guidelines emphasize site selection and operational security. Annexes I and II are checklists which will help you determine your security needs.



## Chapter II. Site Selection Guidelines

### *Need for Security Criteria*

From a security point of view, proper site selection is the most important initial step to provide adequate protection. It is the intent of this e-Book to bring to the attention of all responsible personnel the wide range of security matters that should be addressed and integrated into the site selection process for new office buildings and existing buildings.

Because of car bombings there are new criteria for site selection on a worldwide basis. Regardless of the geographic process, thereby preparing for what might happen during the life of the building or its occupancy. We have all seen how quickly a benign security situation can evolve into a significant threat to facilities. It is only prudent to incorporate adequate security measures based on an evaluation of the existing threat and the potential for a higher future threat level to protect your employees and visitors for the long term. It will be evident from the factors highlighted that security considerations will impact on operational matters. The implication of this fact may be greater in some geographic regions than in others and will certainly affect some more seriously than others. Where this is the case, it is incumbent on all interested parties to evaluate potential damage while engaged in the site selection process and balance it against security requirements. If, in high threat areas, many of the suggested key criteria cannot be met the firm should consider choosing another, more secure location.

Everyone involved in site selections should be aware of the following suggested criteria for facilities.



***New Office Building (for exclusive or predominant operational control)***

*Topography*

Site ideally should be situated at the high point, if any, of a land tract, which makes it less vulnerable to weapons fire, makes egress/ingress more difficult and easier to detect or observe any intrusions.

*Siting*

Site should be located away from main thoroughfares and provide for the following:

- 100 feet minimum setback from the building to perimeter walls and vehicular entrances to the building.
- Sufficient parking space for personnel outside the compound in a secure area within sight of the building, preferably, immediately adjacent to the compound.
- Sufficient parking space for visitors near the site but not on the site itself.
- Sufficient space to allow for the construction of a vehicular security control checkpoint (lock-type system), which would allow vehicles to be searched, if deemed necessary, and cleared without providing direct access to the site.
- Sufficient space to allow for the construction of a pedestrian security control checkpoint (gatehouse/booth) to check identification, conduct a package check or parcel inspection or carry out visitor processing before the pedestrian is allowed further access to the site. If a need for a thorough check of purses and briefcases, as well as items carried on a person may be required, sufficient space for a Walk-Through Metal Detector (WTMD) should be considered. Walking through a WTMD is less intrusive than a personal search or even one conducted with a hand-held detector.
- Sufficient space for construction of a 9 foot outer perimeter barrier or wall.

*Environmental Considerations*

Site should be located in a semi-residential, semi-commercial area where local vehicular traffic flow patterns do not impede access to or from the site.



### ***Existing Office Building***

The following security considerations for high-rise buildings are listed in order of preference as the availability of local facilities dictate:

- A detached (free-standing) building and site entirely occupied and controlled by you.
- A semidetached office building that is entirely occupied by you.
- A non-detached office building that is entirely occupied and controlled by you.
- A detached (free-standing) office building in which the uppermost floors are entirely occupied and controlled by you.
- A semidetached office building in which the uppermost floors are entirely occupied and controlled by you.
- A non-detached office building in which the uppermost floors are entirely occupied and controlled by you.
- A detached (free-standing) office building in which the central floors are entirely occupied and controlled by you.
- A semidetached office building in which the central floors are entirely occupied and controlled by you.
- A non-detached office building in which the central floors are entirely occupied and controlled by you.
- A detached (free-standing) office building in which some floors are occupied and controlled by you.
- A semidetached office building in which some floors are occupied and controlled by you.
- A non-detached office building in which some floors are occupied and controlled by you.

### ***Common Requirements***

Both new and existing office buildings should be capable of accommodating these security items:

- Floor load capacity must be able to maintain the additional weight of public access control (PAC) equipment (ballistic doors, walls, windows), security containers, and disintegrators and shredders, if needed.
- Exterior walls must be smooth shell, sturdy, and protected to a height of 16 feet to prevent forced entry.
- Building must be conducive to grilling or eliminating all windows below 16 feet.



The previously-listed criteria should be adopted to provide satisfactory protection for employees and visitors. If the site is found to be deficient in some areas, attempt to resolve those deficiencies by instituting security measures that will negate the deficiencies. Professional security and/or engineering assistance should be considered to address unique situations.

At a minimum, the following general security measures should be incorporated into planning designs: perimeter controls, grillwork, and shatter-resistant film for windows, public access controls, package search and check, secured area, provisions for emergency egress, and emergency alarms and emergency power.

### *Standards of Design for Site and Building Security*

This section establishes the minimum physical security standards to be incorporated in the design of facilities.

The intent is to provide protection for assets, personnel, property, and customers; ensure that consistent security measures are used at various locations; and ensure design integrity and compatibility of all elements of security with the architecture of the site.

Labor-saving and state-of-the-art security system components and assemblies should be used in all U.S. activities operating overseas, provided they can be maintained locally and there are spare parts available locally.

For manufacturing plant and laboratory facilities, security equipment such as closed-circuit television (CCTV) cameras and monitors, intercoms, card readers, and special glass protection, should be considered. Special care should be taken to verify the vendor's references, especially as they pertain to the quality of alarms, a visit should be made to the central station to observe the professionalism of the operation. Design, purchase, and installation should be coordinated through your architect. Bear in mind, and make provisions for, the cost of maintenance on your security equipment. In some locations overseas, security equipment may be less expensive and more reliable than guards who receive relatively low pay and little training.



*Security Design Objectives*

In designing business or activity sites, roadways, buildings, and interior space, the following functional security objectives should be achieved:

- Physical and psychological boundaries (signs, closed doors, etc.) should establish four areas with increasing security controls beginning at the property boundaries. The areas are defined as:
  - perimeter - property boundaries;
  - exterior - lobbies/docks;
  - interior - employee space; and
  - restricted - laboratories, computer rooms, etc.
  
- Vehicular traffic signs should clearly designate the separate entrances for trucks/deliveries and visitors and employee vehicles. Where feasible – control points should be provided near the site boundaries. Sidewalks should channel pedestrians toward controlled lobbies and entrances.
  
- Avoid having unsecured areas where there is no one nearby with responsibility for the function of the areas.



## Chapter III. Exterior Protection

### ***Perimeter Security***

*Walls, Fences, Berms, etc.*

The overall design for perimeter security should consider using natural barriers, fencing, landscaping, or other physical or psychological boundaries to demonstrate a security presence to all site visitors.

If the threat is considered to be high at free-standing facilities, there should be a smooth faced perimeter wall or combination wall/fence, a minimum of 9 feet tall and extending 3 feet below grade. The wall or fence may be constructed of stone, masonry, concrete, chain link, or steel grillwork. However, if space limitations and local conditions dictate the need, any newly constructed wall should be designed to prevent vehicle penetration, and should use a reinforced concrete foundation wall, 18 inches thick with an additional 1-1/2 inches of concrete covering on each side of the steel reinforcement, and extending 36 inches above the grade. This type of wall is designed to support three wall toppings: masonry, concrete, or steel picket fencing. The toppings should be securely anchored into the foundation wall. If a picket fence is used instead of a wall, the upright supports should be spaced at least 9 feet apart so that the fence, if knocked down, can not be used as a ladder. In addition, intrusion alert systems can be used to enhance perimeter security.

In cases where the above standards of construction are neither feasible, fiscally prudent, nor required by the threat, alternative methods offering comparable protection can be used. These alternatives should maximize the use of locally available materials and conditions to take advantage of existing terrain features or by the creative use of earth berms and landscaping techniques such as concrete planters.

Inside the perimeter barrier, the building should be set back on the property to provide maximum distance from that portion of the perimeter barrier which is accessible by vehicle. The desirable distance of the setback is at least 100 feet depending on the bomb resistance provided by the barrier.



At facilities with less than optimum barriers, or at locations where the terrorist threat or building location increases the vulnerability to vehicular attack, bollards\* or cement planters can be used to strengthen the perimeter boundary. At walled or fenced facilities with insufficient setback, bollards or planters can be installed outside the perimeter to increase the setback of the buildings.

(In any event, whether at a walled facility or a non-walled one as discussed below, the design and placement of bollards or other anti-vehicular devices should be considered in the early planning stages. It would prevent having impenetrable gates connected by easily penetrated walls, or necessitate relocating because local authorities forbid the construction of required barriers.)

### ***Non-walled Facilities Barriers***

In locations without perimeter wall protection, buildings should be protected with bollards, cement planters, or any other perimeter protection device. Such devices should be placed in a manner as to allow the maximum distance between the building and the roadway and/or vehicle access area. They should be positioned to impede vehicular access to lobbies and other glassed areas that could be penetrated by a vehicle (i.e., low or no curb, glass wall or door structure between lobby and driveway). Driveways should be designed and constructed to minimize or preclude high-speed vehicular approaches to lobbies and glassed areas. (There may be local ordinances that make placement of these devices illegal or ineffective.)

A positive and concerted effort should be made to contact local host country law enforcement or governmental authorities and request that they prohibit, restrict, or impede motor vehicles from parking, stopping, or loading in front of the facility.

In high threat locations, if local conditions or government officials prohibit anti-vehicular perimeter security measures and your business is either the sole occupant of the building or located on the first or second floor, you should consider relocating to more secure facilities.

\* A device constructed to protect against a ramming vehicle attack. They are deployed in lines around a perimeter for anti-ram protection, or to provide supplemental control of vehicle traffic through permanent checkpoints when other means are not practical or effective.



## ***Building Exterior***

### *Facade*

The building exterior should be a sheer/smooth shell, devoid of footholds, decorative lattice work, ledges, or balconies. The building facade should be protected to a height of 16 feet to prevent access by intruders using basic hand tools. The use of glass on the building facade should be kept to an absolute minimum, only being used for standard size or smaller windows and, possibly, main entrance doors. All glass should be protected by plastic film. Consider the use of Lexan(tm) or other polycarbonate as alternatives to glass where practical.

### *External Doors*

Local fire codes may impact on the guidance presented here. As decisions are made on these issues, local fire codes will have to be considered.

Main entrance doors may be either transparent or opaque and constructed of wood, metal, or glass. The main entrance door should be equipped with a double-cylinder dead bolt and additionally secured with crossbar or sliding dead bolts attached vertically to the top and bottom of each leaf. All doors, including interior doors, should be installed to take advantage of the door frame strength by having the doors open toward the attack side.

All other external doors should be opaque hollow metal fire doors with no external hardware. These external doors should be single doors unless used for delivery and loading purposes.

Should double doors be required, they should be equipped with two sliding dead bolts on the active leaf and two sliding dead bolts on the inactive leaf vertically installed on the top and bottom of the doors. A local alarmed panic bar and a 180 degree peephole viewing device should be installed on the active leaf.

All external doors leading to crawl spaces or basements must be securely padlocked and regularly inspected for tampering.



## *Windows*

The interior side of all glass surfaces should be covered with a protective plastic film that meets or exceeds the manufacturer's specifications for shatter-resistant protective film. A good standard is 4 millimeter thickness for all protective film applications. This film will keep glass shards to a minimum in the event of an explosion or if objects are thrown through the window.

Grillwork should be installed on all exterior windows and air-conditioning units that are within 16 feet of grade or are accessible from roofs, balconies, etc. The rule of thumb here is to cover all openings in excess of 100 square inches if the smallest dimension is 6 inches or larger.

Grillwork should be constructed of 1/2 inch diameter or greater steel rebar, anchored or imbedded (not bolted) into the window frame or surrounding masonry to a depth of 3 inches. Grillwork should be installed horizontally and vertically on center at no more than 8 inch intervals. However, grillwork installed in exterior window frames within the secure area should be spaced 5 inches on center, horizontally and vertically, and anchored in the manner described previously. Decorative grillwork patterns can be used for aesthetic purposes.

Grillwork that is covering windows designated as necessary for emergency escape should be hinged for easy egress. All hinged grillwork should be secured with a key operated security padlock. The key should be maintained on a cup hook in close proximity of the hinged grille, but out of reach of an intruder. These emergency escape windows should not be used in planning for fire evacuations.

## *Roof*

The roof should be constructed of fire-resistant material. All hatches and doors leading to the roof should be securely locked with dead-bolt locks. Security measures such as barbed, concertina or tape security wire, broken glass, and walls or fences may be used to prevent access from nearby trees and/or adjoining roofs.



## ***Vehicular Entrance and Controls***

### *Vehicular Entrance*

Vehicular entry-exit points should be kept to a minimum. Ideally, to maximize traffic flow and security, only two regularly used vehicular entry-exit points are necessary. Both should be similarly constructed and monitored. The use of one would be limited to employees' cars, while the other would be used by visitors and delivery vehicles. Depending on the size and nature of the facility, a gate for emergency vehicular and pedestrian egress should be installed at a location that is easily and safely accessible by employees. Emergency gates should be securely locked and periodically checked. All entry-exit points should be secured with a heavy duty sliding steel, iron, or heavily braced chain link gate equipped with a heavy locking device.

The primary gate should be electrically operated (with a manual back-up by a security officer situated in an adjacent booth). The gate at the vehicle entrance should be positioned to avoid a long straight approach to force approaching vehicles to slow down before reaching the gate. The general technique employed is to require a sharp turn immediately in front of the gate.

In addition to the gate, and whenever justifiable, a vehicular arrest system can be installed. An appropriate vehicle arrest system, whether active, a piece of equipment designed to stop vehicles in their tracks, or passive, a dense mass, will be able to stop or instantly disable a vehicle with a minimum gross weight of 15,000 pounds traveling 50 miles per hour.

### *Vehicular Control*

#### General

All facilities should have some method of vehicle access control. Primary road entrances to all major plant, laboratory, and office locations should have a vehicle control facility capable of remote operation by security personnel with automated systems.

- At smaller facilities, vehicle access control may be provided by badge-activated gates, manual swing gates, etc.
- Site security should be able to close all secondary road entrances thereby limiting access to the primary entrance. Lighting and turn space should be provided as appropriate.



*Control Features*

Primary perimeter entrances to a facility should have a booth for security personnel during peak traffic periods and automated systems for remote operations during other periods.

Capabilities are:

- Electrically-operated gates to be activated by security personnel at either the booth or security control center or by a badge reader located in a convenient location for a driver;
- CCTV with the capability of displaying full-facial features of a driver and vehicle characteristics on the monitor at security control center;
- An intercom system located in a convenient location for a driver to communicate with the gatehouse and security control center;
- Bollards or other elements to protect the security booth and gates against car crash;
- Sensors to activate the gate, detect vehicles approaching and departing the gate, activate a CCTV monitor displaying the gate, sound an audio alert in the security control center;
- Lighting to illuminate the gate area and approaches to a higher level than surrounding areas;
- Signs to instruct visitors and to post property as required;
- Road surfaces to enable queuing, turnaround, and parking;
- Vehicle bypass control (i.e., gate extensions), low and dense shrubbery, fences, and walls.

***Booth Construction and Operation***

As noted previously, at the perimeter vehicular entry-exit a security officer booth should be constructed to control access. (At facilities not having perimeter walls, the security officer booth should be installed immediately inside the facility foyer.)

If justified by the threat level the security officer booth should be completely protected with reinforced concrete, walls, ballistic doors, and windows. The booth should be equipped with a security officer duress alarm and intercom system, both annunciating at the facility receptionist and security officer's office.



This security officer would also be responsible for complete operation of the vehicle gate. If necessary, package inspection and visitor screening may be conducted just outside of the booth by an unarmed security officer equipped with walk-through and hand-held metal detectors. Provisions for the environmental comfort should be considered when designing the booth.

### ***Parking***

#### *General*

Security should be considered in the location and arrangement of parking lots. Pedestrians leaving parking lots should be channeled toward a limited number of building entrances.

All parking facilities should have an emergency communication system (intercom, telephones, etc.) installed at strategic locations to provide emergency communications directly to Security.

Parking lots should be provided with CCTV cameras capable of displaying and videotaping lot activity on a monitor in the security control center. Lighting must be of adequate level and direction to support cameras while, at the same time, giving consideration to energy efficiency and local environmental concerns.

If possible, parking on streets directly adjacent to the building should be forbidden. Wherever justifiable, given the threat profile of your company, there should be no underground parking areas in the building basement or ground-level parking under building overhangs.

#### *Within Perimeter Walls/Fences*

All parking within perimeter walls or fences should be restricted to employees, with spaces limited to an area as far from the building as possible. Parking for patrons and visitors, except for pre-designated VIP visitors, should be restricted to outside of the perimeter wall/fences.



### *Garages*

For those buildings having an integral parking garage or structure, a complete system for vehicle control should be provided. CCTV surveillance should be provided for employee safety and building security. If the threat of car bombing is extant, consideration must be given to prohibiting parking in the building.

Access from the garage or parking structure into the building should be limited, secure, well lighted, and have no places of concealment. Elevators, stairs, and connecting bridges serving the garage or parking structure should discharge into a staffed or fully monitored area. Convex mirrors should be mounted outside the garage elevators to reflect the area adjacent to the door openings.

### *Exterior Lighting*

Exterior lighting should illuminate all facility entrances and exits in addition to parking areas, perimeter walls, gates, courtyards, garden areas, and shrubbery rows.

Lighting of building exterior and walkways should be provided where required for employee safety and security. Regarding building facades, there should be a capability to illuminate them 100% to a height of at least 6 feet.

Although sodium vapor lights are considered optimum for security purposes, the use of incandescent and florescent light fixtures is adequate. Exterior fixtures should be protected with grillwork when theft or vandalism has been identified as a problem.

For leased buildings, landlord approval of exterior lighting design requirements should be included in lease agreements.



## ***Building Access***

### *Building Entrances*

The number of building entrances should be minimized, relative to the site, building layout, and functional requirements. A single off-hours entrance near the security control center is desirable. At large sites, additional secured entrances should be considered with provisions for monitoring and control.

### *Door Security Requirements*

- All employee entrance doors should permit installation of controlled access system hardware. The doors, jambs, hinges and locks must be designed to resist forced entry (e.g., spreading of door frames, accessing panic hardware, shimmed bolts and/or latches, fixed hinge pins). Don't forget handicap requirements when applicable.
- Minimum requirement for lock cylinders are "6-pin" pin-tumbler-type. Locks with removable core cylinders to permit periodic changing of the locking mechanism should be used.
- All exterior doors should have alarm sensors to detect unauthorized openings.
- Doors designed specifically for emergency exits need to have an alarm that is audible at the door with an additional annunciation at the security control center. These doors should have no exterior hardware on them.

### *Window Precautions*

- For protection, large showroom type plate glass and small operable windows on the ground floor should be avoided. If, however, these types of windows are used and the building is located in a high-risk area, special consideration should be given to the use of locking and alarm devices, laminated glass, wire glass, film, or polycarbonate glazing.
- For personnel protection, all windows should have shatter-resistant film.

(For a more extensive discussion of windows and how to secure them, as well as guidance for securing windows which may be used for emergency exit, see "Windows" on page 18).



*Lobby*

Main entrances to buildings should have space for a receptionist during the day and a security officer at night. The security control center should be located adjacent to the main entrance lobby and should be surrounded by professionally designed protective materials.

The lobby-reception area should be a single, self-sufficient building entrance. Telephones and rest rooms to meet the needs of the public should be provided in this area without requiring entry into interior space. Rest rooms should be kept locked in high-threat environments and access controlled by the receptionist.

Consistent with existing risk level, the receptionist should not be allowed to accept small parcel or courier deliveries routinely unless they are expected by addressee.

*Other Building Access Points*

Other less obvious points of building entry, such as grilles, grating, manhole covers, areaways, utility tunnels, mechanical wall, and roof penetrations should be protected to impede and/or prevent entry into the building.

Permanent exterior stairs or ladders from the ground floor to the roof should not be used, nor should the building facade allow a person to climb up unaided. Exterior fire escapes should be retractable and secured in the up position.

*Construction Activities*

Landscaping and other outside architectural and/or aesthetic features should minimize creating any area that could conceal a person in close proximity to walkways, connecting links, buildings, and recreational spaces.

Landscaping design should include CCTV surveillance of building approaches and parking areas.

Landscape plantings around building perimeters need to be located at a minimum of 4 feet from the building wall to prevent concealing of people or objects.

## Chapter IV. Interior Protection

### *Building Layout*

Building space can be divided into three categories: public areas, interior areas, and security or restricted areas requiring special security measures. These areas should be separated from one another within the building with a limited number of controlled passage points between the areas. "Controlled" in this context can allow or deny passage by any means deemed necessary (i.e., locks, security officers, etc.).

Corridors, stairwells, and other accessible areas should be arranged to avoid places for concealment.

Generally, restricted space should be located above the ground-floor level, away from exterior walls, and away from hazardous operations. Access to restricted space should be allowed only from interior space and not from exterior or public areas. Exit routes for normal or emergency egress should not transit restricted or security space.

### *Walls and Partitions*

Public space should be separated from interior space and restricted space by slab-to-slab partitions. When the area above a hung ceiling is used as a common air return, provide appropriate modifications to walls or install alarm sensors. In shared occupancy buildings, space should be separated by slab-to-slab construction or as described previously.

### *Doors*

Normally, interior doors do not require special features or provisions for locking.

In shared occupancy buildings, every door leading to interior space should be considered an exterior door and designed with an appropriate degree of security.



Stairway doors located in multi-tenant buildings must be secured from the stairwell side (local fire regulations permitting) and always operable from the office side. In the event that code prevents these doors from being secured, the floor plan should be altered to provide security to your space.

Emergency exit doors that are designed specifically for that purpose should be equipped with a local audible alarm at the door and a signal at the monitoring location.

Doors to restricted access areas should be designed to resist intrusion and accommodate controlled-access hardware and alarms.

Doors on building equipment and utility rooms, electric closets, and telephone rooms should be provided with locks having a removable core, as is provided on exterior doors. As a minimum requirement, provide 6-pin tumbler locks.

For safety reasons, door hardware on secured interior doors should permit exit by means of a single knob or panic bar.

### *Other Public Areas*

The design of public areas should prevent concealment of unauthorized personnel and/or objects.

Ceilings in lobbies, rest rooms, and similar public areas should be made inaccessible with securely fastened or locked access panels installed where necessary to service equipment.

Public rest rooms and elevator lobbies in shared occupancy buildings should have ceilings that satisfy your security requirements.

### *Special Storage Requirements*

Building vaults or metal safes may be required to protect cash or negotiable documents, precious metals, classified materials, etc. Vault construction should be made of reinforced concrete or masonry and be resistant to fire damage. Steel vault doors are available with various fire-related and security penetration classifications.



*Elevators*

All elevators should have emergency communications and emergency lighting. In shared occupancy buildings, elevators traveling to your interior space should be equipped with badge readers or other controls to prohibit unauthorized persons from direct entry into your interior space. If this is not feasible, a guard, receptionist or other means of access control may be necessary at each entry point.

*Cable Runs*

All cable termination points, terminal blocks, and/or junction boxes should be within your space. Where practical, enclose cable runs in steel conduit.

Cables passing through space that you do not control should be continuous and installed in conduit. You might even want to install an alarm in the conduit. Junction boxes should be minimized and fittings spot welded when warranted.

***Security Monitoring***

*Security Control Center*

If you have a security control center, it should have adequate space for security personnel and their equipment. Additional office space for technicians and managers should be available adjacent to the control center.

Your security control center should provide a fully integrated console designed to optimize the operator's ability to receive and evaluate security information and initiate appropriate response actions for (1) access control, (2) CCTV, (3) life safety, (4) intrusion and panic alarm, (5) communications, and (6) fully zoned public address system control.



The control center should have emergency power and convenient toilet facilities. Lighting should avoid glare on TV monitors and computer terminals. Sound-absorbing materials should be used on floors, walls, and ceilings. All security power should be backed up by an emergency electrical system.

The control center should be protected to the same degree as the most secure area it monitors.

#### *Controlled Access System*

This type of system, if used, should include the computer hardware, monitoring station terminals, sensors, badge readers, door control devices, and the necessary communication links (leased line, digital dialer, or radio transmission) to the computer.

In addition to the normal designated access control system's doors and/or gates, remote access control points should interface to the following systems: (1) CCTV, (2) intercom, and (3) door and/or gate release.

#### *Alarm Systems*

Sensors should be resistant to surreptitious bypass. Door contact monitor switches should be recessed wherever possible. Surface-mounted contact switches should have protective covers.

Intrusion and fire alarms for restricted areas should incorporate a backup battery power supply and be on circuits energized by normal and emergency generator power.

Control boxes, external bells, and junction boxes for all alarm systems should be secured with high-quality locks and electrically wired to cause an alarm if opened.

Alarm systems should be fully multiplexed in large installations. Alarm systems should interface with the computer-based security system and CCTV system.



Security sensors should individually register an audio-visual alarm (annunciator or computer, if provided) located at the security central monitoring location and alert the security officer. A single-CRT display should have a redundant printer or indicator light. A hard-wired audible alarm that meets common fire code standards should be activated with distinguishing characteristics for fire, intrusion, emergency exit, etc. All alarms ought to be locked in until reset manually.

#### *Closed-Circuit TV (CCTV)*

CCTV systems should permit the observation of multiple camera transmission images from one or more remote locations.

Switching equipment should be installed to permit the display of any camera on any designated monitor.

#### *Hardware*

To ensure total system reliability, only high quality security hardware should be integrated into the security system.

#### *Stairwell Door Reentry System*

In multi-tenant high-rise facilities, stairwell doors present a potential security problem. These doors must be continuously operable from the office side into the stairwells. Reentry should be controlled to permit only authorized access and prevent entrapment in the stairwell.

Reentry problems can be fixed if you provide locks on all stairwell doors except the doors leading to the first floor (lobby level) and approximately every fourth or fifth floor, or as required by local fire code requirements. Doors without these locks should be fitted with sensors to transmit alarms to the central security monitoring location and provide an audible alarm at the door location. Appropriate signs should be placed within the stairwells. Doors leading to roofs should be secured to the extent permitted by local fire code.



*Special Functional Requirements*

Facilities with unique functions may have special security requirements in addition to those stated in this e-Book. These special requirements should be discussed with Corporate Security personnel or a security consultant. Typical areas with special requirements are product centers, parts distribution centers, sensitive parts storage facilities, customer centers, service exchange centers, etc.



## Chapter V. Public Access Controls (PAC)

### *Security Officers and Watchmen*

All facilities of any size in threatened locations should have manned 24 hour internal protection. Security Officers should be uniformed personnel and, if possible, placed under contract. They should be thoroughly trained, bilingual and have complete instructions in their native language clearly outlining their duties and responsibilities. These instructions should also be printed in English for the benefit of American supervisory personnel. If permitted by local law/customs, investigations or checks into the backgrounds of security officers should be conducted.

At facilities with a perimeter wall, there should be one 24 hour perimeter security officer post. If the facility maintains a separate vehicular entrance security officer post, such a post should be manned from 1 hour before to 1 hour after normal business hours and during special events. Security officers should be responsible for conducting package inspections, package check-in, and, if used, should operate the walk-through and hand-held metal detectors. Security officers should also be responsible for inspecting local and international mail delivered to the facility, both visually and with a hand-held metal detector before it is distributed. X-ray equipment for package inspection should be employed if the level of risk dictates.

At facilities with a perimeter guardhouse, the walk-through metal detector could be maintained and operated in an unsecured pass-through portion of the guardhouse. In addition, this security officer could also be responsible for conducting package inspections. When there is sufficient room to store packages at the guardhouse, checked packages should be stored here--new guardhouses should provide for such storage. If package storage at the guardhouse is not feasible, then it should be in shelves in the foyer under the direction of the foyer security officer or receptionist. Generally, security screening and package storage is carried out in the foyer.

### *Security Hardline*

Office areas should be equipped with a "hardline" to provide physical protection from unregulated public access. Protection should be provided by a forced-entry-resistant hardline that meets ballistic protection standards. These standards can be obtained from your corporate personnel or a security consultant. When a security hardline for Public Access Control (PAC) is constructed, the following criteria should apply:

### *Walls*

Walls comprising a PAC should be constructed of no less than 6 inches of reinforced concrete from slab to slab. The reinforcement should be of at least Number 5 rebar spaced 5 inches on center, horizontally and vertically, and anchored in both slabs. In existing buildings, the following are acceptable substitutions for 5 inch reinforced concrete hardlines:

- Solid masonry, 6 inches thick or greater, with reinforcing bars horizontally and vertically installed;
- Solid unreinforced masonry or brick, 8 inches thick or greater;
- Hollow masonry block, 4 to 8 inches thick with 1/4 inch steel backing;
- Solid masonry, at least 6 inches thick, with 1/4 inch steel backing;
- Fabricated ballistic steel wall, using two 1/4 inch layers of sheet steel separated by tubular steel studs;
- Reinforced concrete, less than 6 inches thick with 1/8 inch steel backing.

### *Security Doors*

Either opaque or transparent security doors can be used for PAC doors. All doors should provide a 15 minute forced entry penetration delay. In addition, doors should be ballistic resistant.

The PAC door should be a local access control door, meaning a receptionist or security officer can remotely open the door.

### *Security Windows*

Whenever a security window or teller-window is installed in the hardline, it should meet the 15 minute forced entry and standard ballistic resistance requirements.

### *PAC Entry Requirements*

No visitor should be allowed to enter through the hardline without being visually identified by a security officer, receptionist, or other employee stationed behind the hardline. If the identity of the visitor cannot be established, the visitor must be escorted at all times while in the facility.



*Alarms and Intercoms*

A telephone intercom between the secure office area, the foyer security officer, and guardhouse should be installed. In facilities where deemed necessary, a central alarm and public address system should be installed to alert staff and patrons of an emergency situation. Where such a system is required, the primary control console should be located in the security control center. Keep in mind that alarms without emergency response plans may be wasted alarms. Design, implement, and practice emergency plans.

*Secure Area*

Every facility should be equipped with a secure area for immediate use in an emergency situation. This area is not intended to be used for prolonged periods of time. In the event of emergency, employees will vacate the premises as soon as possible. The secure area, therefore, is provided for the immediate congregation of employees at which time emergency exit plans would be implemented.

The secure area should be contained within the staff office area, behind the established hardline segregating offices from public access. An individual office will usually be designated as the secure area. Entrance into the secure area should be protected by a solid core wood or hollow metal door equipped with two sliding dead bolts.

Emergency egress from the secure area will be through an opaque 15 minute forced-entry-resistant door equipped with an alarmed panic bar or through a grilled window, hinged for emergency egress. The exit preferably will not be visible from the facility's front entrance.

## Chapter VI. Emergency Exit

All facilities should have a means of emergency escape aside from the secure area exit. Positioned appropriately throughout the building should be sufficient emergency exit points to accommodate normal facility occupancy.

All emergency doors should be hollow metal doors (fire doors where appropriate) equipped with alarmed emergency exit panic bars.

Emergency factors regarding windows are described in Chapter III.



## Chapter VII. Communications

### *Communications Facilities*

Satellite ground stations, microwave parabolic reflectors, and communications towers and supports should be located on rooftops, with limited access to the public. Where this is not possible, the equipment should be installed with fences and alarms. Closed circuit television (CCTV) with video recording capability should be considered and included where justified.

### *Communications*

Telephone systems should incorporate an external direct line telephone link for security and life safety independent of the internal telephone network dedicated to the location. This line should feed into the secure area.

Communications considerations should provide radio transmission equipment for communications between security personnel.

Intercom systems should have the capacity to accommodate all remote access control points.

### *Systems Integration*

Security systems in new buildings or buildings undergoing renovation should be installed with distributed wiring schemes that use local telecommunication closets as distribution points. This will provide expansion capability, future networking capability, ease of maintenance, and full function implementation of the security system. At a minimum, the communications link and interface between the sensor, output devices, and computers should include conduit, multi-conductor twisted shielded cable and terminal cabinets. However, recent technology such as fiber-optic cables should be considered in planning the wiring distribution scheme. Data distribution and gathering closets used for security wiring must be secure.



## Certified Security Information e-Books

Where possible, integrate security wiring with other systems such as telephone, paging, energy management, etc. In every case, the design of the communications link should permit ready installation and interconnection of cameras, sensors, and other input-output devices. All life safety equipment and accessories should be Underwriters Laboratory (UL) approved.

Outlying facilities should link security systems to the nearest security control center. All new systems should be compatible with existing systems or the existing system should be replaced with the new system.



## Chapter VIII. Office Security Guidelines

### *General Procedures*

Any employee, but especially the executive, can be a target of terrorist or criminal tactics and forced entry, building occupation, kidnapping, sabotage, and even assassination. Executive offices can be protected against attacks.

The executive office should have a physical barrier such as electromagnetically operated doors, a silent trouble alarm button, with a signal terminating in the Plant Protection Department or at the secretary's desk, and close screening of visitors at the reception and security officer desks in the lobbies and again at the executive's office itself. Secretaries should not admit visitors unless positively screened in advance or known from previous visits. If the visitor is not known and/or not expected, he or she should not be admitted until satisfactory identification and a valid reason to be on site is established. In such instances, Security should be called and an officer asked to come to the scene until the visitor establishes a legitimate reason for being in the office. If the visitor cannot do so, the officer should be asked to escort the visitor out of the building.

Unusual telephone calls, particularly those in which the caller does not identify himself/herself or those in which it appears that the caller may be misrepresenting himself/herself, should not be put through to the executive. Note should be made of the circumstances involved (i.e., incoming line number, date and time, nature of call, name of caller). This information should then be provided to the Security Department for follow-up investigation.

Under no circumstances should an executive's secretary reveal to unknown callers the whereabouts of the executive, his/her home address, or telephone number.

The executive, when working alone in the evening, on weekends, or holidays, should advise Security how long he/she will be in the office and check out with Security when leaving.



*Security in the Office*

American enterprises, particularly those in foreign countries, have been and will continue to be the subject of controversial political and economic issues that can turn their executives and offices into targets for terrorists and criminal actions. Countermeasures against these acts can and should be implemented in the office environment. The following list describes some of the measures that may be useful in improving personal security and safety at the office.

- Avoid working alone late at night and on days when the remainder of the staff is absent.
- The office door should be locked when you vacate your office for any lengthy period, at night and on weekends. Do not permit the secretary to leave keys to the office or desk.
- There should be limited access to the executive office area.
- Arrange office interiors so that strange or foreign objects left in the room will be immediately recognized.
- Unescorted visitors should not be allowed admittance nor should workmen without proper identification and authorization.
- Implement a clean desk policy. Do not leave papers nor travel plans on desk tops unattended.
- Control publicity in high-risk areas. Avoid identification by photographs for news release. Maintain a low profile.
- Janitorial or maintenance activity in key offices and factory areas should be supervised by competent company employees.
- A fire extinguisher, first-aid kit, and oxygen bottle should be stored in the office area.
- The most effective physical security configuration is to have doors locked (from within) with one visitor access door to the office area.
- Where large numbers of employees are involved, use the identification badge system containing a photograph.



*Advice for Secretaries*

A secretary has close knowledge of schedules and company business. He/she should be instructed to maximize security, and the following precautionary measures should be reviewed with him/her:

- Be alert to strangers visiting the executive without an appointment and who are unknown to him/her.
- Be alert to strangers who loiter near the office.
- Do not reveal the executive's whereabouts to unknown callers. Even if the caller is known, the information should be on a need-to-know basis. As a standard policy, take a number where the caller can be contacted. Do not give out home telephone numbers or addresses.
- When receiving a threatening call, including a bomb threat, extortion threat, or from a mentally disturbed individual, remain calm and listen carefully. Each secretary and/or receptionist should have a threatening telephone call checklist which should be completed as soon as possible. A boiler-plate checklist is attached as Annex III.
- Keep executive travel and managers' travel itineraries confidential. Strictly limit distribution to those with a need to know.
- Incinerate, disintegrate or shred notes, drafts, correspondence and any and all material which reveal an executive's travel plans, itineraries, home address and telephone number, invitations and responses thereto or any other data about his/her whereabouts, including information about past trips which could indicate habitual contacts and travel patterns. Do not place such material in trash cans.
- Observe caution when opening mail. A list of things to look for is included in Annex IV. You should post this list in your mail handling facility.

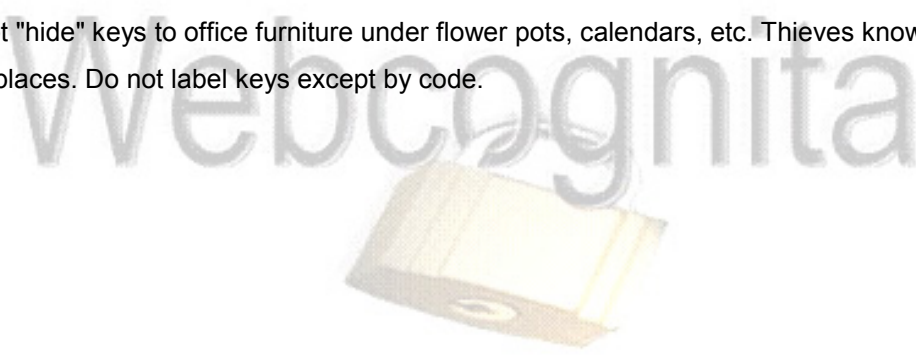
(All persons handling mail should be made aware of the aforementioned basic signs found in Annex IV. The mail handlers should have available an established procedure in the event that any of the above signs are found. It is also important not to accept packages from strangers until satisfied with the individual's identity and the nature of the parcel.)



*Precautions for All*

Money, valuables, and important papers such as passports should not be kept in your desk. Thefts will occur in all offices, even during working hours. Some will be solved, most could have been prevented. The following suggestions will decrease the chance of further thefts:

- Do not tempt thieves by leaving valuables or money unsecured.
- If sharing an office or suite of offices, stagger lunch hours and coffee breaks so that the office is occupied at all times.
- If the office must be left vacant, lock the door.
- Locate desks in a way that persons entering the office or suite can be observed.
- Follow a clean desk policy before leaving at night. Keep valuables and company documents in locked containers.
- Confirm work to be done or property to be removed by Maintenance, outside service personnel, or vendors.
- Do not "hide" keys to office furniture under flower pots, calendars, etc. Thieves know all the hiding places. Do not label keys except by code.



## Chapter IX. Vehicular and Travel Security

### *Vehicle and Travel Security*

Threats of terrorism and kidnapping are serious problems involving all aspects of security management; effective management dictates that available resources be used wisely and concentrated on security weak points. Terrorists are very quick to identify the security vulnerabilities of business, family, and pleasure travel. At their best, protection strategies dealing with vehicles and travel are perhaps the hardest to formulate, and the advantage tends to be with the terrorist. Current statistics indicate that the greatest danger from acts of terrorism occurs while the executive is traveling to or from the office and just before reaching his/her destination.

The inherent security problems of passenger vehicle travel are many. Vehicles are easily recognized by year, make, and model, and the trained terrorist can accurately assess any protection modifications and security devices. Using adequate resources, vehicles can be discreetly followed; therefore, making possible repeated dry runs of potential attacks with very low risk of detection. Under these conditions, different methods of attack can be formulated and tested until success is ensured. While traveling in a passenger vehicle, the executive has limited protection resources upon which to rely and often is dependent on fixed security manpower. This makes it easier for terrorist groups, which are geared to mobility, to ensure numerical superiority.

The attack potential against the executive in travel rests heavily on psychological instability and human weakness. The shock of surprise attack is greatest at points of changing surroundings, crossroads, and when entering or exiting vehicles. These are situations of constant change and points of activity where the executive has a tendency to be mentally off balance. Vehicles are often left in driveways, on streets, at service centers, and other isolated areas with no form of control or protection, allowing easy access to terrorists. Through illegal entry to the vehicle, the terrorist can gain a number of attack points; sabotage with the intent to maim and injure, sabotage with the intent of execution, and sabotage to ensure the success of future attacks. These psychological factors make the vehicle the ideal place to apply scare tactics, warnings, and gain initial control of the executive.



Even though travel problems provide the greatest number of security and psychological variables, there are actions and policies that can be developed to minimize the executive's risk and complicate the terrorist's plans. The basic travel policy can be divided into three areas: (1) Normal Travel Procedures, (2) Vehicle Equipment, and (3) Vehicle Defense Strategy. The following checklists will aid in formulating and evaluating an effective travel security policy.

### *Normal Travel Procedures Checklist*

- The avoidance of routine times and patterns of travel by executives is the least expensive security strategy that can be utilized. The selection of the route should be at the discretion of the executive, not of the chauffeur. Always restrict travel plans to a need-to-know basis.
- Avoid driving in remote areas after dark and keep to established, well traveled roads.
- In high risk areas or when individuals are considered attractive targets, consideration should be given to executives and drivers being trained in antiterrorism strategy and defensive driving. Establish responsibilities and develop contingency plans.
- There should be a simple duress procedure established between the executive and drivers. Any oral or visual signal will suffice (i.e., something that the executive or driver says or does only if something is amiss).
- Never overload a vehicle, and all persons should wear seat belts.
- Always park vehicles in parking areas that are either locked or watched and never park overnight on the street. Before entering vehicles, check for signs of tampering.
- When using a taxi service, vary the company. Ensure that the identification photo on the license matches the driver. If uneasy for any reason, simply take another taxi.
- When attending social functions, go with others, if possible.
- Avoid driving close behind other vehicles, especially service trucks, and be aware of activities and road conditions two to three blocks ahead.
- Keep the ignition key separate and never leave the trunk key with parking or service attendants.
- Before each trip, the vehicle should be inspected to see that (1) the hood latch is secure, (2) the fender wells are empty, (3) the exhaust pipe is not blocked, (4) no one is in the back seat or on the floor, and (5) the gas tank is at least three quarters full.
- Establish a firm policy regarding the carrying and use of firearms. Local laws may prohibit firearms.

*Vehicle Equipment Checklist*

- The executive vehicle designed to meet the terrorist or criminal threat in a high threat area should be a hardtop model with the following special equipment: (1) inside hood latch, (2) locked gas caps, (3) inner escape latch on trunk, (4) steel-belted radial tires with inner tire devices that permit movement even with a flat tire, (5) radiator protection, (6) disk brakes, and (7) an anti-bomb bolt through the end of the exhaust pipe.
- Positive communications can be ensured with a two-way radio or a car telephone.
- It is recommended that the executive vehicle designed to meet the terrorist or criminal threat carry the following safety equipment: (1) fire extinguisher, (2) first-aid kit, (3) flashlight, (4) two spare tires, (5) large outside mirrors, and (6) a portable high-intensity spotlight.
- For additional protection, the vehicle should have an alarm system with an independent power source (an additional battery).

*Vehicle Defense Strategy Checklist*

- Always be alert to possible surveillance; if followed, drive to the nearest safe location, such as police stations, fire stations, or shopping center and ask for help. Carry a mini-cassette recorder in the car to dictate details of a suspect surveillance car such as color, make, model, license plate, description of occupants, etc. It is difficult to make such detailed notes while driving.
- Where feasible, drive in the inner lanes to keep from being forced to the curb.
- Beware of minor accidents that could block traffic in suspect areas; especially crossroads because they are preferred areas for terrorist or criminal activities as crossroads offer escape advantages.
- If a roadblock is encountered, use shoulder or curb (hit at 30-45 degree angle) to go around, or ram the terrorist or criminal-blocking vehicle. In all cases, do not stop and never allow the executive's vehicle to be boxed in with a loss of maneuverability.
- Blocking vehicles should be rammed in a non-engine area, at 45 degree, in low gear, and at a constant moderate speed. **KNOCK THE BLOCKING VEHICLE OUT OF THE WAY.**
- Whenever a target vehicle veers away from the terrorist vehicle, it gives adverse maneuvering room and presents a better target to gunfire.

*Travel Security Suggestions*

The following are general traveling security suggestions:

- Discuss travel plans on a need-to-know basis only. Telephone operators and secretaries should not advise callers and visitors when an executive is out of town on a trip.
- Remove company logos from luggage. Luggage identification tags should be of a type that allows the information on the tag to be covered. Use the business address on the tag.
- Do not leave valuables and/or sensitive documents in the hotel room.
- When sightseeing, observe basic security precautions and refrain from walking alone in known high-crime areas.
- Always have telephone change available and know how to use the phones. Learn key emergency phrases of the country to be able to ask for police, medical, etc.
- Joggers should carry identification.
- Men should carry wallets either in an inside jacket pocket or a front pants pocket, never in a hip pocket. The less money carried the better. Credit cards can be used for most purchases.
- The telephone numbers of the U.S. Embassy or U.S. Consulate, and company employee contact numbers should be carried with employees at all times.
- Always carry the appropriate documentation for the country being visited.
- When traveling, ask for a hotel room between the second and seventh floors. Most fire department equipment does not reach higher to effect rescue and ground floor rooms are more vulnerable to terrorist or criminal activity.
- American-type hotels usually offer a higher level of safety and security inasmuch as they offer smoke alarms, fire extinguishers, safety locks, hotel security, 24 hour operators, English-speaking personnel, safety deposit boxes, and normally will not divulge a guest's room number.
- Choose taxis carefully and at random. Be sure it is a licensed taxi. Do not use independent non-licensed operators.
- Be as inconspicuous as possible in dress, social activities, and amount of money spent on food, souvenirs, gifts, etc.
- Stay in or use VIP rooms or security zones when waiting in commercial airports abroad. Minimize the amount of time spent in airports.
- Confirm arrivals at destinations with office and/or family. Use an itinerary when traveling.
- When traveling internationally, keep all medicine in original containers and take a copy of the prescription.



## Chapter X. Visiting Personnel Protection

### *General Principles*

This chapter provides guidelines regarding security procedures to be implemented during visits of company executives. Guidelines for three levels of threat (minimal threat, moderate threat and high threat) are set forth below along with the factors which determine the level of threat that may exist.

These guidelines should be viewed as tools to assist in organizing and planning visits by company executives or other key personnel. Their implementation will reduce the executive's exposure to terrorist acts, criminal activity, and potential embarrassment.





## Minimal Threat-Factors and Guidelines

### *Minimal Threat Factors*

Factors which should be used by management in determining whether in view of the local security environment a minimal threat potential exists include the following:

- A stable local government;
- Effective law enforcement;
- No significant history of terrorist acts against multinational companies or their executives;
- No previous history of criminal or terrorist acts directed against company executives;
- No significant level of criminal activity (particularly violent crimes such as robbery, kidnapping, murder, and rape);
- No current adverse publicity against the company and no local group activity protesting company policies;
- Other risk factors applicable to the local environment.

### *Minimal Threat Guidelines*

#### Security Coordination

A management-level employee should be assigned as security coordinator. The coordinator's responsibilities consist of implementing the established security guidelines, coordinating all other security aspects of the visit, and serving as the visitor's main contact.

The coordinator should be present at the airport, hotel, and events during arrivals and departures. He/she should ensure adequate security precautions are taken and be present at large public functions.

#### *Air Travel*

- Travel in corporate aircraft is preferable because contact with the general public is limited, but use of commercial airlines is an acceptable alternative provided the airline involved is not considered a likely terrorist target.
- When booking reservations, you should make no reference to the visitor's position.
- Personnel should be available at the airport to handle baggage and expedite customs clearances and local airport formalities, both on arrival and departure. A VIP room should be reserved at the airport for possible use in the event of a delayed departure by the aircraft.

- Time spent at the airport should be kept to a minimum. Public areas should be avoided, if at all possible.
- Use of public transportation to and from airports is not recommended.
- Distribution of travel itineraries should be restricted.

#### **Aircraft Security**

This section applies in the event that corporate aircraft are used.

- The hiring of contract security officers at major international airports to secure the corporate aircraft during stopovers is not necessary provided that the airport has a viable security system.
- The use of contract security officers on a 24 hour basis is necessary in the event that the corporate aircraft uses a remote airfield with limited operations and minimal security or is parked in a remote area of a major airport.

#### **Local Transportation**

- The use of public transportation such as taxis, buses, and subways is not recommended.
- A four-door sedan should be available for use throughout the visit. Care should be taken to ensure that the vehicle is unobtrusive, so as not to bring undue attention to the visitor. The chauffeur or driver, if used, should be bilingual and knowledgeable of the local area and routes to be traveled.

#### **Accommodations**

- Hotel reservations should be booked at a first class hotel located in a low-crime area. Hotel management need not be contacted to provide unusual security or other arrangements for the visitor. A low-key approach is essential to ensure anonymity. Reference to the company or the visitor's position should be avoided.
- Visitors should be pre-registered to avoid being required to check in at the reception desk. The room key should be provided to the visitor immediately upon his or her arrival at the hotel or airport by personnel responsible for coordinating the visit.
- The guest room or suite should be located between the second and seventh floor of the hotel, preferably on a floor with a separate concierge. The room should be away from the public elevator lobby but near an emergency exit.
- Valuables should be stored in accordance with hotel safekeeping provisions.
- Use of a guesthouse or private residence is acceptable as long as it is not located in an isolated area.



*Official Functions and Activities*

- Coordinate all activities and visit sites before the visitor's attendance. The coordinator should obtain guest lists and detailed itineraries, determine emergency evacuation routes, and ascertain the purpose of the function.
- The coordinator should ensure that the function or activity does not subject the visitor to undue risk.
- Official company functions should be on an invitational basis and guests should be required to present their invitations at a reception desk staffed by company personnel before being granted access to the function. The receptionist should match the invitation to the guest list.

*Liaison With Local Authorities*

Prior to a visit by a VIP, you should make contact with the appropriate local authorities to advise them of the upcoming visit and to ascertain whether the current local security environment necessitates an upgraded security posture for the visit.

*Background Data*

An information packet should be prepared before the visit and presented to the executive upon his/her arrival. Information provided should include:

- Emergency telephone contact list, including company personnel (home and office numbers), hospital, police, fire, emergency services, and company doctor;
- Maps of the area;
- Detailed itinerary;
- Availability of company transportation;
- Brief review of current security situation including curfews, government-imposed restrictions, description of high-crime areas to be avoided, and other relevant factors; and
- Explanation of local currency (exchange rates and currency control laws or regulations).

*Other*

- Details of visits by VIPs should be considered company confidential and distribution limited on a need-to-know basis.
- Media coverage, unless requested by the visitor, is unwarranted.



## **Moderate Threat-Factors and Guidelines**

### *Moderate Threat Factors*

Factors which should be used by management in determining whether in view of the local security environment a moderate threat potential exists include the following:

- Stable local government;
- Effective law enforcement;
- Some history of terrorist attacks against multinational companies and/or their executives;
- No previous history of criminal or terrorist acts directed against company executives;
- Upswing in criminal activity, particularly violent crimes with some history of criminal kidnappings for financial gain;
- Some current adverse publicity against the company and potential for nonviolent groups to protest against company policies during the executive's visit.

### *Moderate Threat Guidelines*

#### Unarmed Security Escort

In addition to the guidance set forth in "Minimal Threat Guidelines," an unarmed security escort should be used when a determination is made by management that a moderate threat exists.



## **High Threat-Factors and Guidelines**

### *High Threat Factors*

Factors which should be used by management in determining whether in view of the local security environment a high threat potential exists include the following:

- Unstable or unpopular local government, with terrorist groups actively attempting to bring about its overthrow;
- Ineffective or corrupt law enforcement agencies unable to reduce criminal activity and bring the terrorist problem under control;
- Significant history of terrorist attacks against multinational companies and/or their executives, including bombings, assassinations, and kidnappings;
- Recent history of criminal or terrorist acts or threats against company facilities and/or their executives;
- Widespread criminal activity reaching all elements of local society with emphasis on violent crimes;
- Considerable adverse publicity against company policies and organized local groups that have been leaning toward violence and are planning to protest company policies during the executive's visit;
- Other factors appropriate to the local environment. Asking the consulate regional security officer at the embassy is a good idea.

### *High Threat Guidelines*

#### Recommendation Against Visit

High-threat potential means a significant risk to the well being of the executive. You should strongly recommend against a visit by the executive if a high risk exists. By definition, this category will apply to a limited number of locations, but might vary based on the local situation at a particular point in time. For example, a potential visit might be deemed a moderate risk one month and high risk another because of changes in the local environment.



### *Armed Protective Security Detail*

If the executive cannot be dissuaded from visiting the high threat area, an armed protective security detail should be used.

Specific guidelines for high risk protective details are beyond the scope of this document because of the multiple and various considerations in organizing each individual protective detail.

However, the use of trained security professionals is essential.

The items covered in "Minimal Threat Guidelines", will still have to be addressed when an armed protective detail is required. However, the manner in which relevant tasks are performed may be modified by guidelines issued in regard to the armed details. Some general guidelines are as follows:

- Professional bodyguards dressed in plainclothes and equipped with weapons and two-way radios should accompany the executive at all times. At least one bodyguard should remain in the direct vicinity of the executive whenever potential public contact is envisioned.
- Security personnel should conduct advance surveys of all sites to be visited and be on the scene throughout the executive's visit to the location.
- Security personnel should be assigned to the hotel or residence on a 24 hour basis to ensure that unauthorized individuals do not enter the room or suite. Cleaning staff should be escorted whenever they enter the accommodations. The room or suite should be periodically checked to ensure that contraband (such as a bomb) has not been introduced into the area.
- An escort car or cars should be used on all vehicular movements by the executive to provide a response capacity in the event of an attack or vehicular mishap or breakdown. The escort car or cars should be staffed by at least two security professionals.
- The executive's vehicle should be driven by a security professional trained in evasive or defensive maneuvers. The vehicle should be inspected before use to ensure that explosive devices have not been installed on the vehicle or that the vehicle has not been otherwise tampered with by unauthorized individuals. Use of an armored car, if available, is recommended.
- Public exposure should be limited to the minimum necessary for the executive to complete his or her assignment.



*Group Activities Guidelines*

The exposure created by a number of executives gathering at a single location necessitates some degree of increased security. The following is a list of some general guidelines for use in such group activities:

- The suites should be inspected before occupancy to ensure that no contraband or unauthorized individuals are located in the rooms.
- Security should be provided for corporate aircraft over-nighting at the local airport. Such security may be provided by off-duty uniformed and armed police officers or contract security guards.
- The hotel activity boards should make no reference to the company. Publicity and press coverage should be minimized. A low profile is strongly recommended. Anonymity is a powerful ally of a traveling executive.
- If possible, hotel guest rooms occupied by company personnel should be located in one section of the hotel. Consideration should be given to hiring a security officer to patrol the hallway in the vicinity of the guest rooms and function rooms during hours of darkness or even on a 24-hour basis.
- Access to functions should be controlled to prevent an unauthorized individual from gaining access to the meetings or functions. This can be handled by assigning a member of the meeting staff to serve as a receptionist outside the door. Access can be granted either by personal recognition or by checking identity cards.
- Information packets provided to participants should include the name and telephone number of the staff person responsible for security. Staff personnel should be provided with an emergency contact list, including the telephone numbers of the nearest hospital with an emergency room, ambulance service, police department, and fire department.
- Consideration should be given to leasing pagers to ensure that staff personnel can be rapidly contacted in the event of an emergency.
- Upon the conclusion of the meeting, staff personnel should inspect all guest rooms and function rooms to ensure that no documents, personal effects, or equipment have been left behind by participants.



## Appendix I. Security Survey Checklist

### **General, Preparatory Data**

1. Site name, address, telephone number: \_\_\_\_\_

\_\_\_\_\_

Please fill in the name of the people holding the following positions:

Manager \_\_\_\_\_

Assistant Manager \_\_\_\_\_

Human Resources Manager \_\_\_\_\_

Person responsible for site security \_\_\_\_\_

Number of Employees \_\_\_\_\_

Area Covered/Office Size \_\_\_\_\_

Operating Hours \_\_\_\_\_

### **Function**

2. Survey should include review of theft reports prepared by this site for an appropriate prior period. Where appropriate, has corrective action been taken? \_\_\_\_\_

Do theft reports reflect patterns, trends, or particular problems at this location? \_\_\_\_\_

3. What does site management regard as the most prevalent or serious security problem?

\_\_\_\_\_



4. Does the site maintain items of value, such as works of art, paintings, wall hangings, etc.?

---

5. What are the site's most valuable physical assets?

---

6. Does the location have an employees' handbook or manual or other means of enumerating rules of conduct?

---

Have employees been notified that violation of these rules are grounds for disciplinary action up to and including discharge?

---

Do these rules of conduct include theft of company, customer, and employee property, including information?

---

7. Identify off-site locations that should be included in survey, to include warehouses, offices, storage facilities, etc.

---

Are these locations protected against vandalism and theft? **YES**      **NO**

8. What is the police agency having jurisdiction over the site?

---

Does the plant have a dedicated telephone line to this agency? **YES**      **NO**



Have they been called for assistance in the recent past? **YES NO**

What has been their response?

---

Do they normally include any of our perimeter in their patrols? **YES NO**

If requested, would they?

---

9. Are police emergency numbers readily available to personnel who should have this information? **YES NO**

10. Is information readily available on how to reach the proper agency for assistance with illegal narcotics, bomb threats, obscene calls, etc.? **YES NO**

Do you have a policy of reporting identifiable items of stolen property to the local police for addition to their files, indexes? **YES NO**

11. Some police agencies have a Crime Prevention Unit that responds to invitations to speak on various topics (drugs, rape, etc.) or that may conduct limited security surveys.

Is this service available? **YES NO**

If so, have you taken advantage of it? **YES NO**



**Perimeter Security**

*Lighting Evaluation*

12. Is the perimeter adequately lighted? **YES NO**

13. Does lighting aid or inhibit guards in the performance of their duties? **YES NO**

14. Is lighting compatible with closed-circuit television (CCTV)? **YES NO**

Does it cause monitor to "bloom"? **YES NO**

15. Is the power supply adequately protected? **YES NO**

16. Is lighting properly maintained and cleaned? **YES NO**

17. Are sensitive areas (parking lots, computer areas, stores, storage rooms, shipping/receiving areas) adequately lighted? **YES NO**

18. If an emergency occurred, is the site adequately lighted? **YES NO**

Is the fence line adequately lighted? **YES NO**

In appropriate areas, is glare projection lighting used? **YES NO**



**Security Force**

19. Proprietary? **YES NO**

Contract? **YES NO**

If contract, name of agency and telephone number If proprietary, what is method and source of selection of personnel?

---

20. Are perimeter patrols conducted? Frequency? **YES NO**

---

21. Is an incident log, including alarms/responses maintained? Reviewed daily?  
By Whom? **YES NO**

---

22. Are security personnel used for non-security related duties? **YES NO**

If yes, what duties? \_\_\_\_\_

23. Does site use photo ID cards? **YES NO**

Compatible with access control system? **YES NO**

Who administers it?  
\_\_\_\_\_

24. Are all employees required to show photo ID card upon entry? Is duplicate copy kept on file?  
**YES NO**

25. Are parking decals or other methods of registering employee vehicles used? **YES NO**  
Are privately owned vehicles permitted to park on site? **YES NO**



If so, can an individual reach a vehicle without passing a guard? **YES NO**

26. Does the site have a receptionist in place at all times? **YES NO**

Are visitors required to register? **YES NO**

Are they provided with an identifying badge, and are non-company employees escorted while on the site? **YES NO**

Is visitor identification verified (e.g., vending company ID, etc.)? **YES NO**

***Perimeter Protection***

27. If outside building walls form part of the perimeter, are all doors and windows secured against surreptitious entry? **YES NO**

Can entry be achieved via the roof? **YES NO**

Can hinge pins be removed from doors? **YES NO**

Are all entry/egress points controlled when opened? **YES NO**

***Internal Security***

***Lock/Key Control***

28. With whom does physical and administrative key control rest?

---

29. Is a master key system in use? **YES NO**

How many grandmaster/master keys have been issued? \_\_\_\_\_

Is adequate control exercised over these keys? **YES NO**



30. Is a cross-control system (name versus key number) in use? **YES NO**

What type of numbering system is in use? **YES NO**

Is the entire system, including blanks, inventoried on a regular basis? **YES NO**

Are they stamped "Do Not Duplicate"? **YES NO**

31. What level of management authorization (written?) is required for issuance of keys?

---

32. Identify personnel who are permitted to have keys to perimeter fence, doors.

---

33. Are office/facility keys, particularly masters, permitted to be taken home? **YES NO**

Are keys signed in/out in a daily log? **YES NO**

34. Are locks rotated? **YES NO**

35. How long has the present lock/key system been in use? \_\_\_\_\_

Have keys been reported lost? **YES NO**

What level key? **YES NO**

What is the policy when this happens?

---

36. Is a record of locations of safes and their combinations maintained? **YES NO**



Are combinations routinely changed annually and when an individual who knows one no longer has that need to know? (separation, transfer, retirement) **YES NO**

Are safe combinations, if written, maintained in a secure place? **YES NO**

***Alarms and Electronics***

37. What type, if any, electronic security system is in use here?

---

Do alarms terminate at the site or at an outside central station? **YES NO**

Has service/response been satisfactory? **YES NO**

38. List alarms such as burglar (doors, windows, space (motion)), duress (receptionist, cashier, nurse), other (card access, CCTV, etc.)

---

***Theft Control Procedures***

39. Does the site have a policy of marking items susceptible to theft (calculators, office equipment, hand tools, microwave ovens, TV monitors, VCRs, etc.) so they can be identified as company property? **YES NO**

Describe the extent of the program.

---

Does it include die stamping or etching and painting? **YES NO**

40. Are serial numbers of all items bearing them recorded? **YES NO**

In the event of theft, is this information related to the police for inclusion in stolen property indexes, and for identification and return in case of subsequent recovery? **YES NO**



41. Are trash receptacles periodically inspected to determine whether items of value may be removed from the site via them? **YES NO**

42. Are all store/office supplies, etc., attended when open? **YESNO**

What is the procedure for drawing supplies when no attendant is present? **YES NO**

43. Are telephone records properly safeguarded to prevent unauthorized destruction?  
**YES NO**

Is access to telephone switching equipment (the "frame room") restricted?  
**YES NO**

44. Who performs custodial services - proprietary or contract janitorial people?

---

Is access limited to the office area only? **YES NO**

Are they bonded? **YESNO**

Are they required to wear ID badges? **YES NO**

Are they checked during the performance of their duties? **YES NO**

Are they inspected by guards as they leave? **YES NO**

Are the janitors' vehicles inspected on the way off the property? **YES NO**

How is trash removed from the site? **YES NO**

Are the vehicles used to remove trash inspected on the way off the property? **YES NO**

Do the janitors have access to restricted or sensitive areas? **YES NO**

Are they given office keys (masters?)? **YES NO**

Are they permitted to take these keys off the site with them? **YES NO**



45. How much cash is kept on site? Is it handled at more than one location? **YES** **NO**

How is cash supply replenished? **YES** **NO**

Where is it kept during working hours? **YES** **NO**

Where is it kept after hours? **YES** **NO**

Where are blank payroll checks kept? **YES** **NO**

Where are blank disbursement checks kept? **YES** **NO**

Considering the neighborhood the site is located in, and the amount of cash on site, how do you assess your vulnerability to armed robbery or burglary?

---

Webcognita

***Proprietary/Limited Information***

46. Is there Proprietary and/or Limited data on site? **YES** **NO**

If so, in what form? \_\_\_\_\_

Is it properly marked? **YES** **NO**

Is it stored in a secure location? **YES** **NO**



Are the following locked at the end of the day:

a. Offices? **YES** **NO**

b. Filing Cabinets? **YES** **NO**

c. Desks? **YES** **NO**

47. What are office destruction procedures and file purging for Proprietary data? **YES** **NO**

48. Does the site have a clean desk policy? **YES** **NO**

***Personnel Security***

49. Are any background checks conducted prior to employment? **YES** **NO**

Are previous employment dates verified? **YES** **NO**

Are personnel medical records properly safeguarded? **YES** **NO**

Is security included in the new hire orientation? **YES** **NO**

Is company property (credit cards, ID keys) retrieved during exit interviews? **YES** **NO**

***Emergency Procedures***

50. Do you have a current bomb threat procedure? **YES** **NO**

Who implements it? (searches areas) \_\_\_\_\_

Does the procedure include a checklist for the switchboard operator? **YES** **NO**

51. Is there a contingency plan for acts of violence? **YES** **NO**

A disaster plan? **YES** **NO**



52. If personnel are required to work alone, are they periodically checked by someone to ascertain their well-being? **YES NO**

What means do they have of calling for help in an emergency? **YES NO**

***Computer Security***

53. Are terminated employees immediately separated from the EDP function? **YES NO**

54. Is access to the data center controlled physically, electronically? **YES NO**

Locked when not in use? **YES NO**

55. Is output distributed via user controlled lock boxes? **YES NO**

Is tape library maintained physically separate from machine room? **YES NO**

***Threat Information***

56. Has liaison been established by your office with the American Embassy Regional Security Officer (RSO)? **YES NO**

Is the RSO able to notify you of security threats concerning known terrorist groups active in the area? **YES NO**

Any groups that harbor hatred for U.S. corporations, your company, its manager, and employees? **YES NO**

Anniversary dates that local population or terrorist groups celebrate? **YES NO**

What tactics and activities are practiced or adopted by local terrorist groups that might affect your company, its managers and employees? **YES NO**

57. Do you have sources that will inform you of any political controversy or labor disputes that might impact your operations? **YES NO**



58. Will you provide Security with copies of information that may be detrimental to the company, received as a result of your contacts with the RSO, as well as other sources, including newspaper articles? **YES NO**





## Appendix II. Facility Questionnaire

1. Are there any known groups that harbor hatred for U.S. businesses, managers and employees? **YES NO**

Identify: \_\_\_\_\_

2. What terrorist groups are known to be active in the area?

\_\_\_\_\_

What tactics have these groups been known to use?

\_\_\_\_\_

What is the possibility of a change in these tactics?

\_\_\_\_\_

3. Are there known groups that vocally oppose foreign capitalism or imperialism in the area?  
**YES NO**

Identify:

4. Are there any known groups that vocally or actively oppose the local government that the United States supports? **YES NO**

Identify:

\_\_\_\_\_

5. Is there any current political controversy or labor dispute that we should be aware of?  
**YES NO**



6. Are there any upcoming anniversary dates that the local population or terrorist groups celebrate? Identify:

---

7. Have there been any previous hostage taking or kidnapping incidents, bombings, assassinations, strikes against U.S. businesses or the government, demonstrations, assaults, sabotage against corporate facilities or products, or occupation of corporate facilities in the area?

**YES NO**

Identify: \_\_\_\_\_

8. If there have been previous hostage taking or kidnapping incidents,

a. How were the victims seized? \_\_\_\_\_

b. What was the fate of the hostages? \_\_\_\_\_

c. How much ransom was demanded? \_\_\_\_\_

d. Was it paid? \_\_\_\_\_

e. How were the negotiations handled? \_\_\_\_\_

9. Does the host country prohibit negotiating with hostage takers or prohibit the payment of ransom? **YES NO**

10. Do you consider the local police and intelligence services effective? **YES NO**

11. What are the aims of the local criminals or terrorist groups?

---



What tactics or type of activity by these groups would best further those aims?

---

12. What is the identified groups' capability of carrying out planned activities such as ambush, hostage taking, kidnapping, execution, bombing, etc.?

---

13. In the event of terrorist activity, which organizations, businesses, groups, or individuals would be the most likely targets?

---





## Appendix III. Threatening Phone Call Checklist

**PLACE THIS UNDER YOUR TELEPHONE - BOMB THREAT!**

QUESTIONS TO ASK:

1. When is bomb going to explode? \_\_\_\_\_
2. Where is it right now? \_\_\_\_\_
3. What does it look like? \_\_\_\_\_
4. What kind of bomb is it? \_\_\_\_\_
5. What will cause it to explode? \_\_\_\_\_
6. Did you place the bomb? \_\_\_\_\_
7. Why? \_\_\_\_\_
8. What is your address? \_\_\_\_\_
9. What is your name? \_\_\_\_\_



**WORDING OF THE THREAT:**

Sex of caller: \_\_\_\_\_  
Race: \_\_\_\_\_  
Age: \_\_\_\_\_  
Length of Call: \_\_\_\_\_  
Number at which call is received: \_\_\_\_\_  
Time: Date: \_\_\_\_\_ / \_\_\_\_\_

**CALLER'S VOICE: (Circle One)**

- Calm Nasal
  - Angry Stutter
  - Excited Lisp
  - Slow Raspy
  - Rapid Deep
  - Soft Ragged
  - Loud Clearing throat
  - Laughter Deep breathing
  - Crying Cracking voice
  - Normal Disguised
  - District Accent
  - Slurred Familiar
- If voice is familiar, who did it sound like?

**BACKGROUND SOUNDS: (Circle All That Apply)**

- Voices Street noises
- Crockery Animal noises
- Clear PA System
- Static Music
- Local House noises
- Booth Long distance
- Motor Other
- Factory machinery
- Office machinery



**THREAT LANGUAGE: (Circle One)**

Well spoken Incoherent

(educated) Taped

Foul Irrational

Message read by threat maker

**REMARKS:**

Report call immediately to: \_\_\_\_\_

Phone number \_\_\_\_\_

Date \_\_\_\_\_ / \_\_\_\_\_

Name \_\_\_\_\_

Position \_\_\_\_\_

Phone number \_\_\_\_\_



**HOSTAGE!**

**QUESTIONS TO ASK:**

Who is this? \_\_\_\_\_

Where are you calling from? \_\_\_\_\_

Is this a prank? \_\_\_\_\_

How do I know this is not a prank? \_\_\_\_\_

May I talk to the hostage? **YES NO**

Is the hostage all right? **YES NO**

What do you want? \_\_\_\_\_

**VERY IMPORTANT:**

Will you call back in 15 minutes? **YES NO**

How can I contact you if I have trouble meeting your demands?

\_\_\_\_\_

**EXACT WORDING OF DEMAND:**

Sex of Caller: **MALE FEMALE**

Race: \_\_\_\_\_

Age: \_\_\_\_\_

Length of call: \_\_\_\_\_

Number at which call is received: \_\_\_\_\_

Time: Date: \_\_\_\_\_ / \_\_\_\_\_



## Appendix IV. Letter and Parcel Bomb Recognition Points

### **WARNING!**

#### **LETTER AND PARCEL BOMB RECOGNITION POINTS**

- Foreign Mail, Air Mail, and Special Delivery
- Restrictive Markings, such as Confidential, Personal, Etc.
- Excessive Postage
- Hand Written or Poorly Typed Addresses
- Incorrect Titles
- Titles but No Names
- Misspellings of Common Words
- Oily Stains or Discolorations
- No Return Address
- Excessive Weight
- Rigid Envelope
- Lopsided or Uneven Envelope
- Protruding Wires or Tinfoil
- Excessive Securing Material, such as Masking Tape, String, etc.
- Visual Distractions



# Security Guidelines for American Enterprises Abroad



by  
Alan Pruitt CPP



This Page Intentionally Left Blank





## Certified Security Information e-Books

Creative Commons (cc) Copyright 2007, Alan Pruitt CPP

Webcognita

[www.webcognita.com](http://www.webcognita.com)

Some rights reserved. Creative Commons Attribution – Non-Commercial – Share Alike 3.0

You are free **to share** – to copy, distribute and transmit this work. You are free **to remix** – to adapt this work...under the following conditions: **Attribution**. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work). **Noncommercial**. You may not use this work for commercial purposes. **Share Alike**. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one. Any of the above conditions can be waived if you get permission from the copyright holder (Webcognita). Nothing in this license impairs or restricts the author's moral rights.





**This e-Book is dedicated to the Professional Problem Solver that exists in all of us.**





**Disclaimer**

Alan Pruitt CPP has done his best to give you useful and accurate information, but it's your responsibility to verify all information discussed in this e-Book before relying on it. He doesn't guarantee that the information will be appropriate to your particular situation or even accurate. Laws, procedures and regulation change frequently and are subject to different interpretations. Every state has its own laws as well. Please obtain competent legal or technical advice from the appropriate government agency or legal advisor, before making your own decision.

Alan Pruitt CPP makes no representation or a warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or guaranteed success. Under no circumstance will he be held responsible for economic or non-economic damages resulting from the use or misuse of any furnished documentation or source. Further, he reserves the right to revise this publication and to make changes from time to time in the content hereof, without notice.

For years the world has recognized a need for competent professionals who can effectively manage complex security issues that threaten people and the assets of corporations, governments, and public and private institutions. As the emphasis on protecting people, property, and information increases, it has strengthened the demand for professional managers. To meet these needs, the ASIS International administers the Certified Protection Professional program. Nearly 10,000 professionals have earned the designation of CPP™. This group of professionals has demonstrated its competency in the areas of security solutions and best-business practices through an intensive qualification and testing program. As a result, these men and women have been awarded the coveted designation of CPP™, and are recognized as proven leaders in their profession. Alan was awarded the CPP™ designation in February 2003.



## TABLE OF CONTENTS

Forward.....	7
Chapter I. Introduction .....	8
Chapter II. Site Selection Guidelines.....	10
Chapter III. Exterior Protection .....	
Chapter IV. Interior Protection .....	
Chapter V. Public Access Controls (PAC).....	
Chapter VI. Emergency Exit .....	
Chapter VII. Communications.....	
Chapter VIII. Office Security Guidelines.....	
Chapter IX. Vehicular and Travel Security .....	
Chapter X. Visiting Personnel Protection .....	
Appendix I. Security Survey Checklist.....	
Appendix II. Facility Questionnaire .....	
Appendix III. Threatening Phone Call Checklist.....	
Appendix IV. Letter and Parcel Bomb Recognition Points .....	



## Forward

**E**ffective security precautions require a continuous and conscious awareness of your environment. This is especially true when living in a foreign country where it will be necessary to adapt to new cultures, customs, and laws which, in most instances, are very different from those to which Americans are accustomed in the United States.

The implementation of security guidelines contained in this e-Book could reduce the vulnerability of American private sector enterprises abroad to criminal or terrorist acts. It is recognized that some of the recommended guidelines cannot easily be implemented at existing facilities.

This Webcognita e-Book is *re-purposed* from the original U.S. Department of State Overseas Advisory Council (OSAC) on-line document with the same title. This re-formatted version of the same document is intended to ease readability and encourage use of the information by interested readers.





## Chapter I. Introduction

This e-Book is a compilation of security guidelines for American private sector executives operating outside the United States. This guidance is the product of many years of experience by a cross section of American security practitioners from both the public and private sectors. Obviously, the implementation should be consistent with the level of risk in the country where you conduct business. For the most part the guidelines are for protection in high threat areas. It is recognized that the level of risk varies from country to country and time to time so that you may need to choose among the suggested options or apply the concepts in a manner modified to meet your needs. Since levels of risk can change very rapidly, it is advisable to continuously monitor factors that may impact the risk level. Security precautions must be flexible and dynamic to respond effectively to changing risks. A static, inflexible security posture will almost certainly result in a lack of preparedness or unnecessary expense.

The Department of State has three threat assessment designators: High, Medium, and Low. One of these three threat designators is applied to each country where the United States has diplomatic representation. Threat assessment information is available to the American business community in countries where the United States has diplomatic representation through the Regional Security Officer or Post Security Officer at the nearest U.S. diplomatic post, i.e. Embassy or Consulate. The level assigned to a particular country is determined by an analysis of the political, terrorist, and criminal environment of that country. It is reviewed quarterly by the Department of State and changed when appropriate.

A High Threat country is one where the threat is serious and forced entries and assaults on residents are common, or where an active terrorist threat exists. A Medium Threat country is one where the threat is moderate, with some forced entries and assaults on residents occurring, or where the area has the potential for terrorist activity. A Low Threat country is one where the threat is minimal and forced entry of residences and assault of occupants is not common, and there is no known terrorist threat.

For emphasis again, the guidelines set forth in this publication are generally most appropriate for High Threat areas. One will probably want to moderate them for applications where the risk is lower; or where other considerations preclude their implementation at the level discussed here. In many situations, professional technical security assistance will be required.



## Certified Security Information e-Books

These guidelines emphasize site selection and operational security. Annexes I and II are checklists which will help you determine your security needs.



## Chapter II. Site Selection Guidelines

### *Need for Security Criteria*

From a security point of view, proper site selection is the most important initial step to provide adequate protection. It is the intent of this e-Book to bring to the attention of all responsible personnel the wide range of security matters that should be addressed and integrated into the site selection process for new office buildings and existing buildings.

Because of car bombings there are new criteria for site selection on a worldwide basis. Regardless of the geographic process, thereby preparing for what might happen during the life of the building or its occupancy. We have all seen how quickly a benign security situation can evolve into a significant threat to facilities. It is only prudent to incorporate adequate security measures based on an evaluation of the existing threat and the potential for a higher future threat level to protect your employees and visitors for the long term. It will be evident from the factors highlighted that security considerations will impact on operational matters. The implication of this fact may be greater in some geographic regions than in others and will certainly affect some more seriously than others. Where this is the case, it is incumbent on all interested parties to evaluate potential damage while engaged in the site selection process and balance it against security requirements. If, in high threat areas, many of the suggested key criteria cannot be met the firm should consider choosing another, more secure location.

Everyone involved in site selections should be aware of the following suggested criteria for facilities.



***New Office Building (for exclusive or predominant operational control)***

*Topography*

Site ideally should be situated at the high point, if any, of a land tract, which makes it less vulnerable to weapons fire, makes egress/ingress more difficult and easier to detect or observe any intrusions.

*Siting*

Site should be located away from main thoroughfares and provide for the following:

- 100 feet minimum setback from the building to perimeter walls and vehicular entrances to the building.
- Sufficient parking space for personnel outside the compound in a secure area within sight of the building, preferably, immediately adjacent to the compound.
- Sufficient parking space for visitors near the site but not on the site itself.
- Sufficient space to allow for the construction of a vehicular security control checkpoint (lock-type system), which would allow vehicles to be searched, if deemed necessary, and cleared without providing direct access to the site.
- Sufficient space to allow for the construction of a pedestrian security control checkpoint (gatehouse/booth) to check identification, conduct a package check or parcel inspection or carry out visitor processing before the pedestrian is allowed further access to the site. If a need for a thorough check of purses and briefcases, as well as items carried on a person may be required, sufficient space for a Walk-Through Metal Detector (WTMD) should be considered. Walking through a WTMD is less intrusive than a personal search or even one conducted with a hand-held detector.
- Sufficient space for construction of a 9 foot outer perimeter barrier or wall.

*Environmental Considerations*

Site should be located in a semi-residential, semi-commercial area where local vehicular traffic flow patterns do not impede access to or from the site.