Site Security

Security Training Module for NGOs

Produced for the OFDA/InterAction PVO Security Task Force

By Jan Davis, RedR
drawing on documentation produced by Aline Curran, Jane Swan and Steve Penny

July 1998

Contents

Module Site security

Goal

To enhance the security of residential and work environments so that operational objectives can be achieved with minimal loss and damage to material or injury to personnel.

Learning Objectives

On completion of this module participants will be able to:

- Identify a general approach to site security.
- Assess the suitability of sites from a security point of view.
- Identify potential threats to residency and workplace sites.
- Recommend and make changes to improve site security.
- Manage the security of different sites.

Key Learning Points

The security of a site is related to the profile of an agency - its program aims and activities, visibility, assets and the behavior of agency personnel.

A site and its affiliations (political, ethnic, religious, factional, etc) can influence how an agency is perceived which, in turn, affects levels of risk.

Site security is maintained through a series of physical and procedural boundaries.

Site security measures can be taken which do not necessarily compromise an agency's acceptance by parties within an operational area.

Effective site security requires agency managers to arrange training for staff in security procedures and to implement and maintain those procedures in practice.

Circumstances change and site security must be regularly reassessed and revised according to the changes.

1.0 Introduction

In considering measures related to site security outlined in this module it is crucial to select sites and implement measures in relation to the overall security approach that an agency has decided to take. (See "Security Strategies" module). It may be counter productive, for example, to be screened behind high walls and steel security gates if the agency's strategy is to work for widespread acceptance of its presence and activities through transparency and open dialogue. Judgments will need to be made on the impact of such a strategy if it is decided to move towards forms of protection, even if limited, such as the locking of stores at night or the employment of guards. Precautions against simple thieving are acceptable in many societies but they may also give unintentional contradictory signals.

The extent to which a 'security measure' impacts on an agency's profile and, therefore, on the strategy it is aiming to follow must be kept in clear focus when assessing sites for accommodation and work, and when taking steps to enhance 'site security'.

This module will cover security at a variety of sites: residence, office, warehouse, and service distribution points. There are general principles of site selection and management which can be applied to all sites and these are covered in section *2.0 General site security*. Additional site-specific issues are outlined in relevant sections.

2.0 General site security

The desirability of a site for targeting may be reduced by lowering the profile of the agency, limiting or lowering the profile of assets, and by fostering good relationships. Vulnerability may be reduced by making access more difficult through the establishment and enforcement of procedures, the strengthening of physical boundaries and equipment, and the use of guards and guard dogs. There will be a compromise between heightening physical security and maintaining a low profile.

2.1 Site selection

Site selection should be based on the agency's security strategy. Factors to consider include the neighborhood, affiliations related to the site, accessibility, susceptibility to hazards and the nature and suitability of the physical space. The extent to which access in and out of the site is controlled will influence how you are perceived. A more fortress-like site, for example, may not contribute to an image of ready access and open relationships.

It is useful to observe what security measures the local community take: barred windows, security fences, exterior lighting, guards and guard dogs. Extensive precautions may indicate either a high level of security awareness or a high crime rate and the reason needs to be investigated. Note what security measures are commonly accepted and, therefore, will not look out of place if implemented by the agency. Norms for local counterparts might provide a good guide or minimum standards.

Site location should also take into account the risks associated with travel between residence, agency office and work sites. For various reasons it will normally be desirable to limit travel distance and time by choosing locations close to each other. Exceptions to this might be when working in insecure areas during the day and returning to living accommodation in safer areas at night. Under varying circumstances it may sometimes be better to stay put than to risk travel. It will be necessary to find a balance between travel and site associated risks.

Once selected, it is important to continually assess and re-evaluate the suitability of a particular site in the context of changing circumstances.

Example

A medical agency providing support in a conflict zone might choose to both live and work in a local hospital to provide an efficient service and, perhaps, to show solidarity with those directly affected. Security of staff will depend on a number of considerations including their acceptance by all parties to the conflict which, in turn, will be influenced by the perceived neutrality and impartiality of the agency and the hospital. Various factors and circumstances such as night-time violence, intensity and proximity of the conflict, *unpredictability of individual combatants, and so on, may dictate how safe it is to stay overnight or use the hospital as a working base. The level of risk associated with the site and, therefore, the security measures taken are likely to vary over time.*

Be aware, therefore, that it may be necessary to change the location of where you live or work depending on the security situation at the time and the security strategy adopted by the agency.

Site evaluation checklist

- Neighborhood: level of crime (statistics); proximity to potential targets; proximity to clandestine hideouts; proximity to safe havens, proximity to politically or military significant buildings.
- Affiliations: the predominant group of people in the area (ethnicity, religion, class, political faction); landlord, past tenants, immediate neighbors and their affiliations.
- Accessibility: single/multiple route access; road condition; surfaced/unsurfaced; wide or narrow; one-way or two-way traffic (two-way is preferable); ease of access or egress from the site; density of traffic and parked vehicles; local transport. Dense vehicle and pedestrian traffic helps criminals or those surveying a site to maintain anonymity.
- Services: water and electricity.
- Lighting to illuminate the site and surroundings.
- Trees and vegetation that might provide cover for intruders.
- Susceptibility to hazards: fire, flood, landslide, strong winds.
- Physical space: single vs multi-tenant, enough space to accommodate needs (vehicles, fuel, equipment, relief materials).
- Physical structures: type, quality, condition and strength of buildings, perimeters, access points.
- Multiple physical boundaries.

Physical and procedural boundaries

Access to a site is controlled through a series of physical and procedural boundaries, or layers. Each boundary is a stage through which any would-be intruder must pass to gain access. They may be physical (a wall), physical and psychological (a low perimeter hedge), or procedural (security checks), or a combination of these. Keep in mind these different barriers when evaluating sites. Clearly defined perimeters, if only a low hedge or simple fence, have a role to play even if they are not physically going to keep intruders out. Ideally, look to establish a series of boundaries, or multiple layers (such as an outer perimeter wall, gatekeeper, outer wall of building with barred windows, receptionist, inner office) which will provide several lines of defense against potential intruders.

2.2 Physical boundaries

The physical boundary checklist can be used when selecting a site or when evaluating an existing site.

Physical boundary checklist

- Well defined perimeter to mark the extent of the property.
- Quality and strength of walls and fences.
- Multiple layers.
- Quality and strength of walls, roof, doors and windows.
- Number and location of windows, doors and gates. Two access points are generally advisable.
- Visibility around the site: clear lines of sight, space free of obstacles, lighting.
- Potential safe havens within the site: inner room with strong door, basement, access to the roof.
- Potential for modifications and the ease with which they can be made: stronger perimeter and gates, lighting, clearance of obstacles, blast walls, bomb shelters, etc

Perimeter security

The outer perimeter is usually the property line marking the extent of the site. The inner perimeter is usually the exterior of the buildings within the site - office, store or residence. A visible outer perimeter is recommended even if it is only a low hedge. The outer perimeter has a psychological and legal significance since any unauthorized person crossing the perimeter becomes an intruder.

Outer perimeter barriers include:

- Natural vegetation/hedges: marks the property line but only useful as a deterrent if thick and/or thorny. Established thorn bush fences can provide effective barriers.
- Picket and chain link fences: offers a view beyond the perimeter and does not provide intruder cover.
- Solid fences: wooden fences can be breached relatively easily and provide cover for intruders.
- Solid block, stone or brick walls: relatively difficult to breach; limits the view out of the site; provides potential cover for intruders.

A perimeter barrier is only as strong as the gate and gate posts. Therefore, to be effective, the gate must complement the type of barrier. For example, a solid wooden or metal gate is suitable for a solid fence or wall, assuming the gate is well supported and has an appropriate lock.

Consider having an emergency exit, or weakened wall to drive through, as an escape route through the rear of the property.

Inner perimeter barriers can comprise:

- Grilles over windows and other openings of significance made up of solid steel bars spaced 150mm (6 inches) apart and supported by horizontal bars to give sufficient rigidity. Bars should be embedded up to 75mm (3 inches) into the walls or frames on either side of openings. Alternatively, bars can be bent and passed through the wall and secured internally. Sufficient grilles should be hinged and provided with an emergency release to provide adequate fire exits.
- Grilles can also be installed behind doors to reinforce the door or provide extra security if the door is weak.
- Primary locks: the main lock on a door with handles.
- Auxiliary locks: usually deadbolts without handles.

Adequate fire alarms and exits should be provided in a building protected by grilles and locked doors. Keep strict control of keys on all exterior locks (see *Checklist for keys* in section 2.2). Do not hide keys outside the house. Burglars know to look under the mat or plant pot.

Guards

Guards provide both a physical and procedural boundary. They require a clearly defined area in which to operate and appropriate equipment: flashlights, whistles, batteries, boots, raincoats, distinctive clothing, and shelter. They should be trained to follow defined security procedures encompassing incident response and reporting. Due care and attention should be paid to the conditions under which guards and guard dogs work. Not only is this for clear welfare reasons but also to foster loyalty and maintain efficiency.

2.3 Procedural boundaries

Physical boundaries are complemented by procedures which establish security conscious patterns of behavior. Procedures determine who should have access to what, when and under what circumstances. Access to vulnerable points should be restricted through clear standard operating procedures (SOPs). SOPs may need to be modified as tension, or risks, increase or decrease. Access to keys, confidential or sensitive information (on computers or in hard copy files), cash, and security significant personnel (storekeepers, senior managers) may need to be carefully controlled.

Checklist for vulnerable points

- Who and what may be vulnerable and why?
- Who needs access and how do they achieve access?
- Who else might want access and for what reasons?
- How might unauthorized access be gained?
- What are the vulnerable aspects of the agency's organizational style or security strategy which might permit unauthorized access?
- How might unauthorized access be made more difficult?

Checklist for keys

- Who has access to keys, when and what for?
- How and where are keys kept?
- Where are copies kept?
- Could the unauthorized copying of keys take place?
- What happens when a key is lost or goes missing?

Procedural boundaries also encompass informal arrangements between personnel. They include:

- Keeping each other informed (e.g. expected time of return from the store).
- Looking out for and checking on each other.
- Radio checks and the responsible use of a radio network.
- Accompanying each other on site inspections (e.g. night-time checks).
- Checking the guard(s) (e.g. on duty, awake, in trouble).
- Checking on windows, doors, locks.
- Discussing and preparing behavior in an emergency.
- Looking out for and acting upon suspicious behavior.

Record keeping is an important security procedure, both formal and informal (security awareness):

- Inventory controls at warehouses, stores, and distribution sites enable checks to be made on equipment and materials.
- Visitor records can aid in incident investigations and the signing someone in and out of a site establishes a psychological boundary.
- Records of who delivered what and when can help track the movements of personnel, equipment and material.
- Awareness of the presence of people: anyone who is not normally present or acts suspiciously.
- Awareness of the presence of objects: maintain a tidy site to make it easier to spot anything out of the ordinary. Arrange furniture to give a good view of the site.

It is also important to maintain a record of security related incidents - from petty crime to threats to employees. These should be reviewed and shared, where appropriate, with others whose security may be similarly at risk. A reciprocal arrangement should allow you to share others records of incidents.

2.4 Security alarms

Security alarms have various functions:

1. Detection of an intruder.
2. Reporting of the intrusion.
3. Creation of discomfort (loud high pitched sound) for the intruder.

Desirable features of an alarm system:

- Operation on the local electricity supply with rechargeable battery back-up.
- Time delay to allow for arming and disarming without activating the system.
- Manual activation of the alarm by means of fixed or mobile panic switches. Panic switches can be positioned for the use of guards, office staff, storekeepers, etc.
- Easy to install and maintain.

A fire alarm installed in a building should have a distinctly different sound to a security alarm and occupants should know the difference through having practiced intruder and fire drills.

2.5 Security lighting

Exterior security lighting has two functions:

- To deter intruders.
- Aid observation.

Exterior lighting can be an important deterrent against intruders. Install a standby generator where power failures are commonplace. In locations where there is no mains electricity supply it can be well worth installing and running a night-time generator to provide security lighting.

Security lighting may comprise standard outside lighting for normal illumination enhanced by floodlights connected to the alarm system which come on automatically when the intruder alarm is activated. A manual switch should allow for independent switching of the floodlights.

2.6 Shelters and allied passive security measures

Safe haven

In locations where there is a possibility of forced entries and direct assaults on staff it may be expedient to make provision for a safe haven within a residence or office. A safe haven is a strengthened or purpose built room within a building where the occupants can take refuge. The aim is to be able to remain safe for at least a brief period whilst assistance is summoned or the attackers flee.

Requirements of a safe haven:

- Substantial walls, roof and door.
- Strong deadbolt lock.
- Optical door viewer (spy-hole in the door).
- Radio communications, if possible.
- Bottled water.
- Toilet buckets.
- First aid kit.
- Secondary escape route, if possible.

Building protection

In certain conflict situations agency staff occupying a building can be vulnerable to snipers, direct attack or cross-fire. It may, therefore, be necessary to take protective measures to shield occupants from small arms fire, shelling or aerial bombardment.

The following points should be considered when modifying a building to withstand attack:

- Stone or fired brick walls are only bullet and splinter-proof if they are at least 0.45m thick.
- 'Sand' bags are often used to provide protection. Sand bags may burst if overfilled. Therefore, only fill sand bags about three-quarters full of earth, or sand.
- Significant numbers of sand bags placed in upper storeys may overload a floor.
- Shored ceilings will strengthen a room.

External walls of buildings can be reinforced by building sand bag walls either inside or outside the building. Placing sand bags on the inside of the building does not make it obvious that the building is protected in this way and, therefore, does not give unintentional messages to external observers.

However, sand bags on the inside reduces the available internal space. Internal walls can also be reinforced with sand bags to give further protection. A door height sand bag wall in front of the doorway obscures the view inside when the door is opened and protects from incoming fire.

Clear plastic shatter resistant film can be placed over windows to protect occupants from flying glass. If clear film is not available then glass windows can be taped. Boards can also be placed in front of windows to protect from rifle fire and shrapnel from incoming rounds landing near the building.

Shelters

A shelter (sometimes called a bolt hole) is designed to protect from small arms fire and nearby shell blasts. It is not designed to withstand a direct hit. Various designs of shelter are shown in figures 1 to 11.

Building a shelter inside a building has the advantage that occupants do not have to expose themselves to danger whilst making their way to an external shelter. The shelter should be in the basement, if possible, as the ground floor should withstand the collapse of the building. If there is no basement then build the shelter in a ground floor room and provide extra support for the ceiling. Whereas a ground floor room or basement will make a better shelter than upper floors there is a risk of being trapped under a building collapse. Therefore, keep emergency digging tools in each room used as a shelter.

Features of a shelter:

- Blast wall in front of the entrance.
- A 1.2m deep x 0.7m wide trench as long as required. Alternatively, if it is not feasible to dig, build sand bag walls at least 3 to 4 bags thick at the bottom to similar dimensions as the trench.
- Support the trench with timber or steel sheets secured in place by vertical poles.
- Place suitable roof supports (tree poles, angle iron, railway lines) across the top of the trench or sand bag walls. On the supports place corrugated iron sheeting and a 0.5m depth of compacted earth or sand bags to form a protective roof.
- Outside shelters should have a blast wall and sand bag tunnel to protect the entrance.

If external underground shelters cannot be built due to rocky or saturated terrain then above ground shelters can be constructed from 40 gallon drums filled with earth or sand, sand bags and similar roofing materials as given above.

A shelter should contain the following equipment and supplies:

- Radio communications.
- A form of lighting.
- Bottled water.
- Tinned food.
- Toilet bucket.
- First aid kit.
- Fire fighting equipment.
- Digging equipment.

3.0 Residential security

3.1 Residence location

When choosing somewhere to live, refer to the *'Site evaluation checklist'* given in section *2.1 Site selection*. There is clearly a balance between keeping a low profile and establishing good relations with neighbors and those associated with the residence. Living in the "agency" part of town can have advantages and disadvantages. A case study illustrates the importance of thinking through the consequences of living in particular areas of a town.

Case study

During a civil war in a central African country an expatriate NGO water engineer worked in a conflict zone during the day but, for security reasons, returned to the capital for the night. He decided that he would prefer to live in an area of the city away from the concentration of expatriate housing. His aim was to associate with people from the same tribe that he was working with during the day. These people generally opposed the incumbent government. A house was located which was rented from a local landlord.

At dusk a few weeks later he and his girlfriend left the house to drive to a nearby market. They were only a few yards down the road when they saw an army 'security' patrol some distance ahead. Without warning the patrol opened fire on the vehicle. Thinking they mistook him for someone else he put his head out of the window and shouted "Don't shoot, I am an American!" The firing continued and he was fortunate enough to reverse and escape the area to find safety at one of the houses in the expatriate area of town. Luckily, the only injury was a superficial bullet wound sustained by his girlfriend.

On investigation of the incident it transpired that the undisciplined army patrol were in the habit of regularly roaming the area to steel from the people who they labeled as 'the enemy'. It was not in the soldiers' interest to have an outsider witnessing such activities and, therefore, they decided to drive him out.

In taking the decision to live in the area, the water engineer not only heightened the risk to himself and his girlfriend but also to the landlord, his neighbors and the people with whom he associated. After the incident he left the country.

Access

Assaults, muggings and kidnappings often take place close to a victim's residence on leaving or returning home. Therefore, have several alternative access routes to vary daily routines and avoid predictable patterns. Ideally, have two entrances/exits. Avoid dead-end and narrow one-way streets.

Vehicle parking

Vehicles may be stolen or targets for vandalism or sabotage. Have a secure parking area for vehicles within physical boundaries. A lockable garage within a perimeter wall is the most suitable but a drive within a walled compound is often all that is possible but acceptable. In areas of increased threat it may also be necessary to employ a guard. Avoid parking a vehicle on the street.

Cluster housing

It can be advantageous for members of the same agency, or colleague agencies, to live in close proximity to each other:

- Observations of suspicious activities in the area can be shared and others can be warned of specific incidents or streets to avoid.
- Vehicles can travel in convoy to and from work or transport can be shared.
- Travel for evening socializing is reduced and so also the potential risks.
- It may be easier to maintain radio contact with VHF hand held sets within a smaller geographical area.
- In times of heightened insecurity one house can be designated as a safe haven for all staff in the area and particular measures taken to improve security at the one dwelling.
- Knowing you are close to friends can maintain confidence and provide reassurance in times of crisis.

3.2 Type of residence

Apartments

In a town there may be a choice between an apartment and a single dwelling. Each have their advantages and disadvantages but an apartment may provide better protection against criminal activity. However, in some cases vehicles may be more vulnerable if no secure area is provided or guarded.

When deciding on an apartment consider the following:

- It can be more difficult for an intruder to gain access to an apartment than a single dwelling, especially one on a higher floor.
- Avoid apartments on the first or second floor which can be accessed from the street, trees, tall vehicles, or porch roofs. Objects can also be accurately thrown up to second floor level.
- Avoid apartments above the reach of the local rescue services who may not be that well equipped to tackle fires above about the seventh floor.
- An apartment can assist the occupier to maintain a low profile through a certain degree of anonymity.
- Who else inhabits the apartment block? Neighbors are very close and, if inclined, can quickly assist in an emergency.
- Access to an apartment must be well controlled by a door-keeper, locks, electronic devices, or similar.
- It is usually relatively cheaper to improve security in an apartment than a single dwelling.

Building modifications

In certain circumstances it may be necessary to modify dwellings to improve security. This should be taken into consideration when selecting the type of residence and checked under the leasing arrangements. Use the *Site evaluation checklist* in section 2.1 to determine possible modifications. In addition, consider the possibility of providing a strengthened refuge within the building designed to protect from potential threats. Depending on the potential threats, this may be a safe haven from assaults on residents or a blast shelter to protect from shelling or bombing - see section *2.6 Shelters and allied passive security measures*.

3.3 Moving in

It is advisable to take a range of security precautions after moving into a new residence. The measures taken will clearly depend on the level of threat. The following list is a guide:

- Register all residents with the appropriate responsible authorities: agency security coordinator and embassy.
- Test alarms and repair or replace as necessary. Change all exterior locks on taking over a building for the first time. It may be possible to change only the lock cylinders rather than all the locks.
- Install an optical viewer in solid external main doors.
- Obtain fire and safety equipment including fire extinguishers, first-aid kit, matches, candles, flashlights with spare batteries, radio with spare batteries, water storage containers, camping cooker and suitable fuel.
- If thought prudent, maintain an emergency store of tinned food, drinks, and bottled water.
- All residents, including domestic staff, should know how to use all the emergency equipment.
- Familiarize yourself with neighbors and their associates to be able to identify strangers in the area.
- Join an alert-calling system with friends and neighbors or start a system if one does not exist.
- Familiarize yourself with the emergency services telephone numbers and how well they operate. If you do not speak the local language then learn key phrases and/or identify someone who can communicate with the emergency services, if necessary.
- Recruit dependable guard(s) through recommendations you can trust.
- Draw up a security map of your neighborhood - see the checklist.

Neighborhood security map checklist

- Walk and/or drive around the neighborhood to orient yourself.
- Drive around at night when the area can look different.
- Note the layout of streets, especially one-way and dead end streets.
- Identify other aid agency housing.
- Identify 'safe havens' (trusted neighbors) in the event of a security incident.
- Familiarize yourself with the route to the nearest emergency hospital.
- Locate the nearest police station or alternative responsible authority that can be called upon in the event of an emergency.

3.4 Domestic staff

If you hire domestic staff then their security and your security are closely linked. It is important to have confidence in each other, especially if working together in an insecure environment. There are various procedures that can be taken to safeguard the interests of the agency, yourself and the staff.

Whenever possible recruit staff who have been employed and recommended by a friend, another reputable agency or neighbor. Take the time to check references with the referees concerned. It may be necessary to obtain a translation from a trusted employee who speaks the language.

All domestic staff should be briefed on security procedures and updated as circumstances change.

Security briefings should cover:

- Security related responsibilities.
- Maintaining security awareness.
- Incident response and reporting procedures.
- Emergency telephone numbers or use of a radio in an emergency.

Avoid discussing security sensitive issues that could be overheard by domestic staff unless of direct relevance to the staff concerned.

4.0 Office security

4.1 Office location

Refer to section *2.1 Site selection* and the associated *Site evaluation checklist* when deciding on the location of an agency office.

Pay particular attention to the following:

- Distance between the office, other agencies, field locations and staff member residences.

- Routes between the office, other agencies, field locations and staff member residences and the associated risks along those routes.

- Secure parking for agency vehicles. Street parking should be avoided.

- Location and accessibility of safe havens, e.g. police station, embassy, government buildings, etc. where staff members can seek safety in case of an emergency.

- Location of airport for medical or emergency evacuation.

- The condition of neighboring buildings - avoid neighborhoods with abandoned and rundown buildings which might attract criminal activity.

- Type and nature of business conducted in the location - try to avoid a site that is adjacent to potential targets of demonstrations, crimes and/or acts of terrorism (political organizations/individuals, military personnel, financial institutions, etc.).

4.2 Type of office

Multi-tenant vs single-tenant buildings

There are numerous types of office from a city center multi-storey tower block to a tent. In most cases the choice will be between a multi-tenant or single tenant building. From a security point of view, each have there advantages and disadvantages.

Multi-tenant

In general, there is safety in numbers but not always. It very much depends with whom you are sharing the building. It is imperative to get to know the other occupants and the landlord, to the greatest extent feasible, *prior* to signing a lease:

- Are any of the existing tenants other humanitarian or U.N. organizations?
- Have any of them been specific targets of crime or acts of terrorism? If so, in what way and why?

- Would it be possible and *feasible* to enter into a security cooperation agreement with any of them? (Seriously consider whether such an agreement would be a benefit or a burden -financial or otherwise - to your organization).
- Who are the other tenants and the landlord (whether on site or off). Is there any reason why any of them might be the specific targets of crime or acts of terrorism? For example, does the building also house:

  - a bank or other institution which handles/stores large quantities of cash?
  - an organization or individual with well-known political, criminal or military ties?

  - any individual or organization/company with a high national or international profile such as the extremely wealthy, famous or controversial?

- How security conscious are the other tenants and the landlord?

  - How many entrances are their to the building and are they guarded?
  - Are the doors and windows *kept* locked?
  - Who has access to the building and how? Photo I.D? Card keys?
  - How often are the locks changed/card keys re-programmed?
  - Are visitors screened and escorted?

  - If guards are employed, how are they alerted? Silent alarm at the reception area or a general alarm that is audible throughout the building?

  - Are the lobby and parking areas monitored by closed circuit television (CCTV)?
  - Are the emergency exits kept unobstructed from the inside and locked from the outside?

- Who hires/pays for security guards and other security measures such as alarms, window bars, etc. in the common areas? The landlord or all tenants? How cooperative are they?

- Will it be possible to locate your office(s) on the third to seventh floors? (First and second floors are more accessible to illegal entry while anything above the seventh may be out of reach of fire and emergency equipment).
- Surveillance of a particular target is sometimes more difficult in a multi-tenant building. However, controlling access to those who might cause you harm may be more difficult due to poor visitor screening procedures and increased difficulty in getting to know the many legitimate occupants.

Single-tenant

The primary benefits to a single-tenant dwelling are that they allow the occupant to have complete control over the building's security, especially access control and visitor screening procedures. On the down side, smaller, single-tenant dwellings are generally not designed with security in mind. You will be less likely to find a single-tenant building that already contains fire escapes, CCTV, etc., and that will increase the security costs to your organization considerably - costs that would normally be shared by other occupants in a multi-tenant building. Also consider that you will be housed on the ground floor, but not required to locate above the seventh. You and your staff will make easier surveillance targets in a single-tenant dwelling, yet *detecting* surveillance will be facilitated by the fact that it will be easier to recognize who belongs in the area.

Site Security

Building structure

Whether you choose to house the office in a multi-tenant or single-tenant building, there are some considerations to be made regarding the structure itself:

- Age of the building - newer sites are likely to have improved plumbing, wiring, insulation, etc.
- Quality of exterior doors, windows and locks - solid core doors? double-paned, shatter resistant glass? electronic/magnetic locks?
- Number and quality of emergency exits - fire escapes, fire doors, interior window latches/locks, etc.
- Sufficient lighting - are the lobby, hallways, stairwells, parking areas and building exterior well lit?
- Overall construction - this is particularly important in regard to natural hazards. Ensure you identify the location and have access to the building's main electrical switch and gas and water shut-off valves.
- Depending upon the vulnerability of the building and geographical location there may be a few additional considerations:
    - *Earthquakes* - avoid all-brick construction; look for cracks in walls and particularly the foundation; look for buildings attached to foundation via bolts through the sill (this may require professional inspection).
    - *Floods* - ensure the building, including basement, is built above flood level.
    - *Hurricanes* - stay away from the ocean; avoid wood and/or thatch construction; insist on shatter-resistant windows and shutters.
    - *Lightening* - avoid the tallest building; check the lightening rod(s).

Perimeter security

Seriously consider another building if the site falls short on perimeter security. If it proves difficult or impossible to locate a sound building in an acceptable neighborhood that already has good perimeter security then it will be necessary to spend the funds to improve the perimeter boundary prior to moving in. You will have little or no power to improve overall building construction or the neighborhood, but there are measures which can be taken to improve perimeter security. Refer to section *2.2 Physical boundaries* and *2.3 Procedural boundaries* for details on perimeter security.

Alarms

Prior to moving into a new building ensure that intruder and fire alarm systems are in place (see section *2.4 Security alarms*). In addition to intruder and fire alarms also consider a silent trouble alarm with a button suitably located (e.g. at reception). Give careful thought to whether local police should be summoned or security guards/employees should respond to the alarm.

4.3 Office security survey

To assist in making the final important decision in selecting an office it is useful to summarize the choices using a security survey checklist. This survey should be designed as a simple but thorough checklist that details a site's security assets, excesses and deficiencies at a glance to aid in the organization's decisions. Which office:

- meets most requirements?
- has the greatest security assets?
- has the greatest security deficiencies?
- has deficiencies that can be lived with and/or improved?
- will cost the most to improve?

An office security survey can be accomplished fairly quickly with a little practice, particularly the second and third times around and provides a useful checklist. After the office is selected and occupied the survey should be conducted annually as security, personnel and mission requirements are likely to fluctuate over time.

A sample format for a survey is included as an appendix. The survey covers both office selection and office security management.

4.4 Office security management

This section will concentrate primarily on the human factor - what can staff do to improve office security.

A little common sense can go a long way to improving office security and the safety of personnel. The following suggestions take very little time and effort and generally cost nothing - unless of course, you choose to ignore them.

Site Security

- Close and lock interior doors and windows when the office is empty, even for short periods of time. Establish a daily office locking up procedure with clearly defined staff responsibilities.
- Stagger lunch hours and coffee breaks so that the office is occupied at all times during working hours.
- Avoid working alone at night and on weekends. If it is necessary to do so ensure all doors (including building entrance) and windows are kept locked and that a colleague or partner is informed of your whereabouts and expected time of return home.
- Arrange the office so that persons entering and leaving the office can be observed.
- Store all confidential files and sensitive materials under lock and key.
- Important papers and travel plans should never be left on unattended desk tops.
- Never store personal valuables in the office.
- Never leave keys in or on your desk. Keep them with you or return them to a key safe.
- Never think it will be OK to "hide" keys or other valuables under flower pots, calendars, false drawer bottoms etc. Thieves know all the hiding places.
- Do not label keys except by code.
- Never share computer or other access codes with anyone and change your passwords frequently.
- Avoid passwords that incorporate important personal dates and names of loved ones, including pets. The most difficult passwords to decipher are those that incorporate a combination of letters and numbers.
- Be careful of what you say in *all* communications - telephone, fax, E-mail and regular post. Unauthorized monitoring is common in many places throughout the world.
- Arrange and keep office interiors tidy so that strange or foreign objects left in the room will be immediately recognized. Avoid clutter and clean the office nightly.
- First aid kits and fire extinguishers should be stored throughout the office area, and checked/ maintained regularly. Instructions on their function and use should be clearly posted.
- All staff members should avoid individual identification through photographs in the local media. Even if the organization is receiving positive press it is preferable to keep a low profile.
- Staff members should be instructed to avoid taking the same routes and departure/arrival times on the way to and from the office.
- To the extent feasible, office hours and/or individual work schedules should be staggered allowing staff members to arrive and leave at different times on different days in a seemingly unpredictable manner.
- All staff members should be fully informed of office security measures and procedures including, but not limited to:
    - visitor access controls
    - employee identification procedures
    - key control
    - security alarms
    - location of emergency exits
    - fire and evacuation drills
    - location and use of fire extinguishers and first aid kits
    - location and purpose of safe havens
    - bombs and bomb threats

Visitor access control and employee identification

The most elaborate security devices in the world will not protect office personnel or property if thieves are invited in through the front door. Visitor monitoring is important even if the office is located in a single-tenant building and there are no more than a handful of employees. In multi-tenant buildings it will be even more important to adhere to access controls than in a small single-tenant office. Therefore, give careful consideration to the following measures.

- Managers must set an example for the other employees - their seniority should not exempt them from security procedures.

- All keys to the building and interior office(s) should be strictly controlled, and any staff member, no matter how senior, should be held accountable for lost or loaned keys in accordance with the organization's policy on key control (many organizations require the employee to cover the costs of changing/reconfiguring the locks, particularly after the second or third offense).

- Stolen or lost keys must be reported immediately, and the locks changed or reconfigured.

- Keys must be collected immediately from any employee who has been suspended or terminated. When in doubt, change or reconfigure the locks.
- All visitors should be accompanied while on the premises. Some organizations require visitors to leave a driver's license or other form of identification with the guard or receptionist.
- Workmen without proper identification and authorization should not be admitted under any circumstances.

- Always confirm with a company contracted to perform tasks what work is to be done, including property to be removed by maintenance or outside service personnel. Ensure that staff know what kind of work is to be carried out.

- Janitorial and maintenance activities in key offices should be supervised by competent employees.
- There should be limited access to the manager's office.

Unauthorized entry

No matter how stringent the security measures and procedures a determined criminal may still gain access to the office. This is one reason why it is imperative for *all* employees and not just the guards and receptionist to monitor who comes and goes. Regardless of your position within the office, be proactive with regard to security:

- If you see an unknown visitor, and you feel that it is safe to do so, ask the person directly what his or her purpose is on the premises and politely explain visitor procedures.

- If you do not feel that it is safe to confront him/her directly, notify a security guard or the manager.

- Nobody should be permitted into offices containing cash or sensitive documents without authorization and supervision, unless it is required for his/her job function.
- Do not try to reason with anyone who is violent, irrational or armed. Notify a security guard or the manager immediately and leave the area for a safe place.

Security of documents and cash

Documents of a sensitive nature (political or security related) should be locked away when not in use. An office should have a safe of adequate size for cash and sensitive documents located in an inner secure room. The location of a safe should not be generally made known. Fix a safe to the floor for added security. The number of a combination type safe should only be known by those who need to use it.

In a highly insecure environment where evacuation or relocation is a possibility, keep sensitive documents separate from other paperwork so that they can quickly be picked up and taken when leaving the premises.

Front line security

If guards are employed they are likely to be mainly responsible for outer perimeter security. Some may work within the building providing additional protection. However, many organizations will employ no guards at all, others will employ only one or two. Regardless of how many guards are employed, or contracted from a security company, they will have little or no knowledge of the activities of the agency office. Guards will make up only a small part of your front line security. Agency office staff will bear a substantial responsibility for effective security. Their daily tasks will include:

- dealing with the public
- screening visitors
- answering the telephones
- making appointments
- arranging travel plans and daily schedules.

It is essential that staff receive office security training and understand the agency approach to security. Staff should be encouraged and given the opportunity to voice their opinions and observations regarding breeches in security, even if this challenges a manager's directives and actions. The following are recommendations for office staff:

- Always be alert to and report any breeches in office security, including but not limited to:

    - Strangers loitering near the office.
    - Unfamiliar vehicles - particularly service vans - parked near the office.
    - Service personnel with or without an appointment.
    - Doors and windows that are unlocked.
    - Emergency exits that are obstructed.
    - Unfamiliar objects anywhere in the office.
    - Colleagues who do not arrive at work as scheduled.

- Carefully follow visitor access control and employee identification procedures. Never feel that it is inappropriate or 'not your place' to challenge senior staff members and/or visiting dignitaries regarding these procedures. Explain to them that you are just doing your job. Bear in mind the safety of secretaries and receptionists who are more likely to become the victims of inner-office security incidents even if they are not the intended targets.

- Be alert to strangers visiting senior staff members without an appointment and who are unknown to you, even if they have identification.

- Never permit a visitor into the interior offices, regardless of their status or whether or not they have an appointment and identification, without first alerting the person(s) they came to see.

- Never permit anyone into the offices of senior staff members if the staff members are not in attendance themselves.

- Keep appointment schedules, travel itineraries and other personal information such as whereabouts, place of residence, etc. of other staff members confidential. Limit distribution only to those who need to know on an emergency basis and only with the consent of the staff member concerned.

- Be wary of unusual telephone calls, particularly those in which the caller does not identify him/herself or if you suspect that the caller is misrepresenting him/herself. Do not immediately put these calls through to the office. Instead, gather as much information from the caller as you can and take careful notes. Then put the caller on hold while you explain the situation to your manager.

- Observe caution when opening mail. Do not open it if it seems unusual. Refer to the following section on *Bomb threats*.

4.5 Bomb threats

The majority of bombs are either carried in through the front door or sent through the post. They may be preceded by a threatening telephone call. Visitor access control is the best method of prevention for the explosive that is 'carried in.'

Parcel bombs

Be wary of any items or packages that seem unusual:

- Excessive weight in ratio to size and/or listed contents.

- Excessive postage for the weight (terrorists are less likely to go to the post office for accurate weight/postage measurements).
- Wires, string, tape, rubber bands attached in unusual/inappropriate locations, especially if they appear to compress the contents.

- A peculiar smell (many explosives smell similar to almonds or shoe polish).
- Oily stains or discoloration.
- Conspicuous restrictive marks, such as Personal, Confidential, etc.
- Missing return address or one that is different from the postmark.
- Incorrect spelling of name or address.
- Foreign mail or special delivery, if not expected.

If a package is suspicious do not touch it but place in the corner of a room. If it has already been opened try to retain evidence such as handwriting or typing paper and postal marks. Do not place suspicious packages in water as this can weaken the packaging and cause a compressed device to detonate. Open the windows and evacuate the building. Inform the appropriate authorities but do not use a radio in close proximity to the suspected device as radio waves could possibly trigger certain devices.

Telephoned threats

A bomb threat may be received by telephone. All personnel, particularly those who regularly answer the phones, should be instructed in what to do if a bomb threat call is received. Do not hang up - immediately try to inform someone else in the office upon receiving a threatening call, by note or gesture. Keep the caller on the phone and try to determine the following critical information:

- Where the bomb is located.
- When it will explode.
- What it looks like.
- What will make it go off.
- How it can be dealt with safely.
- Why it was planted.
- Who planted it.

Speak slowly and clearly in a calm and soothing voice. Slow and steady communication will prolong the conversation, help to calm an agitated bomber and go a long way toward alleviating your own tension. Follow these guidelines:

- *Write down* what is said.

- Listen closely for anything that will give away the identity of the caller and pay particular attention to his/her voice quality, such as male/female, old/young, high/low pitch, calm/agitated, accents, speech impediments, coughing, etc.

- Listen for anything that will give away the location of the caller - background noises, such as music, radio/television, machinery, traffic, nature sounds, other voices, etc.

- Inform the caller that the building is occupied, and the detonation of a bomb could result in serious injury or death to many innocent people, including mothers and children**.** (Many bombers do not actually wish to cause injuries or deaths. If told that the building is occupied or cannot be evacuated in time, the bomber may be willing to give more specific information about the bomb, including purpose, location, components and time/method of detonation).

- Ask the caller who they are (some will actually provide this information - either because they are not very bright or else they want to be caught).
- Ask the caller whether the call is truly being addressed to the correct office and whether it is a real threat (he/she may have the wrong number/organization and/or the call could be just a sick prank).

- Ask the caller his/her reason for the threat, and listen sympathetically whether it's a personal problem, money demand, anger at an individual or organization, mental disturbance, religious/political grievance, etc.

- Do not give in or offer to comply with any threats.

- Ask the caller to whom the threat is specifically directed (the organization, an individual staff member, a government, etc.).

- Even in a threat situation always bear in mind that politeness and courtesy can help in extracting as much information as possible. The caller may well be your best, if not only, source of information regarding the bomb.

- It might be worth asking the caller to call back or leave a number where he/she can be reached, especially if it is gauged that the caller wishes to prolong the threat. Explain that you want to discuss the problem and address the issues of concern to the caller with senior staff.

4.6 Personal staff details

The more an organization knows about its staff members, the more appropriately it can respond to assisting those staff members. Some organizations require all employees to submit personal information forms, some ask for them on a voluntary basis and some do not ask at all. A minimum amount of information on each staff member and family will help to gauge the kind of mutual assistance that can be given, or might be needed, in an emergency. A manager will need to decide on what information is desirable, or reasonable to request, in any particular situation:

- *Personal*: name, current address and telephone, nationality, passport number, date/place of issue and expiration, date of visa expiration.
- *Home country or region*: if working away from home then address and telephone in home country/town/village; and name, address, telephone and relationship of emergency contact.
- *Medical*: age, blood type, sex, medications and important medical conditions/physical limitations of staff member and family.

- *Security information*: list any skills that could assist the office in an emergency, such as emergency medical training, first aid training, foreign language skills, truck/bus/aircraft/watercraft operators license, military experience, psychological counseling, security training, etc.

All personal information should be recorded in confidential files kept in a secure place.

5.0 Warehouse security

Staff: storekeepers, guards, laborers

Procedures: stock control, dispatch notes, waybills, spot checks, etc

Physical boundaries: outer perimeter, warehouse types (Solid, purpose built, modified, Rubb type shelter, etc)

6.0 Service distribution point security

Refer to the guidelines given in section 2.0 *General site security*. In addition to these general guidelines there are security precautions specific to particular sites which are detailed in this section.

6.1 Refugee camps

The following security guidelines on working in refugee camps should be adapted to each particular camp situation:

- Locate the agency camp office adjacent to a main access route.
- It is recommended to reside some distance away from the camp.
- Check in and out of a camp with the relevant authorities (camp manager, agency manager, refugee representative) so that a clear record can be kept of who is on the site.
- Familiarize yourself with the layout of a camp on arrival and as it expands or evolves over time. Take note of signs, agency flags and logos, landmarks such as prominent trees, service centers, any police or military presence.
- Keep informed about what is happening in and around the camp. Attend the various camp meetings and listen to drivers, and local and refugee representatives.
- Be alert and maintain security awareness.
- Whenever possible, travel with someone else, especially when walking through the camp.
- If there is a radio network then keep tuned in and carry your portable VHF set with you. Do not be careless and leave the radio lying around.
- Avoid disputes. It can be easy to get drawn into an argument or become associated with a dispute simply through close proximity. Do not take sides and withdraw from any dispute.
- Refugees are subject to the laws of the host country. Do not interfere with the due process of law.
- Know your place in a security plan for the camp. In particular, establish an evacuation plan and guidelines covering evacuation: signal for evacuation, continuation or closure of services, evacuation route(s), convoy arrangements, etc.

6.2 Food distribution sites

6.3 Health care centers

7.0 Crowds and mobs

A crowd is a peaceful gathering of people who have a lawful reason for gathering. A mob is an aggressive group of people with a purpose:

- to inflict violence - to kill.
- to escape - from a perceived threat such as shooting or fire.
- to acquire - looting or robbing.

A major concern is to prevent a crowd becoming a mob.

7.1 Crowd control

Crowd control relies upon:

- Pre-empting the situation - plan based on reliable information and be aware of potential problems.
- Defusing the situation if it begins to get out of hand - negotiation and continual talking.
- Containing the situation quickly - which may mean calling in the police or army.

There are several reasons why a crowd should get out of control:

- People do not know what is happening or they do not approve of what is happening.
- There is a feeling that time is running out.
- The crowd is disorderly and has no internal structure.
- People are tired and/or desperate.
- There is organized stirring up of the crowd.
- Poor planning and lack of sensitivity to social and cultural issues.

Crowds are unavoidable in many relief situations. Manage crowds by:

- Planning in advance.
- Meeting with representatives of the people concerned and discussing the objectives.
- Organizing into smaller groups.
- Getting people to sit down in small groups.
- Providing physical needs - shelter, water, sanitation, first aid.
- Enlisting people (community leaders) from the group to assist with control and to accompany you.
- Keeping people informed.

Have a contingency plan if the situation deteriorates:

- Have assistance on call.
- Ensure a vehicle is available to leave quickly.
- Plan an evacuation route and regularly check that it is still open.

If you are stopped in a vehicle and confronted by a crowd - stay inside, lock the doors and close the windows, drive carefully away from the situation.

Appendices

Office security survey

Note that completion of a survey in all its detail summarizes a range of information which can be used in selecting the best of a number of sites. It is also a record for future reference. Circumstances may change and it may be necessary to move to an alternative site. Having the information in a summarized form can aid in future selection. Regular staff changes are commonplace in humanitarian aid agencies and a record of sites and the decision making process can greatly assist future managers.

Photographs accompanying the survey report provide an *aide memoir* and further detail. However, be careful that the act of taking photographs does not in itself arouse suspicion and that it is permitted.

1. General information

a. Survey Conducted by:

(1) Name of Individual:
(2) Agency/Organization:
(3) Address:
(4) Telephone/Fax Numbers:
(5) Date of Survey:

b. Previous Survey:

(1) Date
(2) Conducted by:

c. Building Owner/Manager:

(1) Owner:
(2) Address:
(3) Telephone:
(4) Manager/Management Company:
(5) Address:
(6) Telephone:
(7) Attach copy of lease terms.

2. General location analysis

a. Crime

(1) General nature of crime in the area:

(2) Specific areas of city/country considered
the most dangerous:
the most safe:
why?

(3) Most common crimes committed against humanitarian personal and foreigners:

(4) Most common crimes committed against international and humanitarian organizations:

(5) Most common methods in which these crimes are carried out:

(6) Have any crimes been committed against the organization's personnel or property in the past five years?

If so, explain each (or attach copy of the incident reports)

(7) Have any crimes been committed against other humanitarian/ international organizations' personnel or property in the past five years?

If so, explain:

b. Emergency Contacts

(1) List other humanitarian organizations in the area, including address, telephone, fax, name/title of senior resident official:

(2) Provide address, telephone, fax, name/title of contact of appropriate embassies:

(3) Provide address, telephone, fax, name/title of contact of local police department:

explain reliability and response time:

list additional capabilities, e.g. bomb squads, search and rescue, etc:

(4) Provide address, telephone of local emergency medical establishments:

explain reliability and response time:

list additional capabilities, e.g. trauma centers, medivac, etc:

(5) Provide address, telephone of local fire department:

explain reliability and response time:

(6) List and explain any additional emergency services in the area, e.g. severe weather warning systems, bomb shelters, etc.

c. Neighborhood

(1) Attach area map with the following locations clearly marked: office, staff residences, embassies, airport, police/fire departments, hospitals, other humanitarian organizations.

(2) General description of area surrounding the office site for one mile radius (to the extent feasible, describe neighboring businesses, condition of other

buildings, traffic flow, street lighting, etc.):

d. Natural Disasters

(1) List types of natural disasters to which the area is prone:

(2) Attach copy of office contingency plan for dealing with these disasters.

3. Site description

a. Building Specifics (provide photo of building if feasible)

(1) Address:
(2) Floor and ground areas:
(3) Number of floors:
(4) Primary construction material:

b. Description of Windows:

(1) Construction:
(2) Locks:
(3) Grills/Bars:

c. Description of Exterior Door(s):

(1) Number:
(2) Type Construction and thickness:
(3) Locking Mechanism(s):
(4) Grills/Bars
(5) Hours of Operations:
(6) Manned by Guard:
(7) Video surveillance:

d. Description of Heating, Ventilation, Air Conditioning system:

e. Primary power source:

(1) Explain type and reliability of local/primary power source:

(2) Explain number, duration and cause of power outages:

(3) Provide description, condition and location of circuit breakers:

f. Emergency power source

(1) Manufacturer:
(2) Model:
(3) Output:

(4) Location of generator and fuel supply:
(5) Protection afforded both:
(6) Who maintains generator:
(7) Frequency of maintenance:
(8) Date of last test:
(9) Is log maintained concerning usage, tests, repairs, and malfunctions:
(10) What does the emergency generator supply? (check all that apply):

___ Interior Lights
___ Communications Equipment
___ Communications Lighting
___ Perimeter Lighting
___ Building Exterior Emergency Lights
___ Building Interior Emergency Lights
___ General Office Equipment
___ Security Alarms
___ Telephone System

g. Provide description, condition and location of emergency shut-off valves for water and gas:

4. *Occupants*

a. List floors occupied by organization:

b. Non-organization tenants:
(1) Total Number:
(2) List by organization and floor/office:

c. Description of tenants on floors immediately above and below facility being surveyed:
(1) Type of organization/company:
(2) Number of employees:

5. *Perimeter security*

a. Fence/Barrier:

(1) Material:
(2) Height:
(3) Thickness:

b. Gate(s)--including vehicle and pedestrian entrances

(1) Material:
(2) Height:
(3) Thickness:
(4) Hours of Operation:

(5) Manned by Guard:
(6) Video surveillance:
(7) Locks:

c. Parking facilities:

(1) Public or Private:
(2) Hours of Operation:
(3) Manned by Guards:
(4) Video surveillance:
(5) Locks:

d. Alarm System Description (list for each type):

(1) Manufacturer:
(2) Model:
(3) Date Installed:
(4) Maintained by:
(5) Area(s) protected:
(6) Type of sensors:
(7) Location of control panel/monitor(s):
(8) Who monitors system?:
(9) Response time to alarm:
(10) Date of last test and results:
(11) Is a log maintained of system operation, repair, malfunction, suspicious operation, false alarms?:
(12) Who maintains the log?:

e. Perimeter Lighting:

(1) Type(s) of Lighting:
(2) Location of Controls:
(3) Blind Spots:
(4) Power Source:
(5) Attached to Alarm System?:
(6) Description of Street/Path Lighting:
(7) Description of Exposed Power cables to perimeter and exterior building lighting susceptible to tampering/sabotage:

6. Interior safe haven

a. Purpose for safe haven (political unrest, criminal/terrorist activities, etc.):
b. Location:
c. Description:
(1) Area:
(2) Door(s):
(3) Window(s):
(4) Locks(s):
(5) Communications Equipment:
(6) Maximum Occupancy:

7. Access control procedures

a. Public/Visitor Procedure

b. Staff Procedure:

c. Key control system used:

(1) Who controls keys:
(2) Is there a master inventory and control log:
(3) How are keys assigned to office personnel:
(4) Number of keys currently issued to:
____Primary entrances

____Interior offices

(5) Explain missing key policy:
(6) Number of keys currently unaccounted for and why:
(7) Reason and date locks last changed or reconfigured:

8. Fire and safety equipment

a. General:

(1) Name of Fire Marshall:
(2) Date of current fire plan:
(3) Date of last fire drill:
(4) Date fire equipment last inspected:
(5) Date last fire/safety inspection:

b. The facility has the following equipment (check all):

___ Sprinkler system
___ Portable extinguisher
___ Hose reel
___ Standpipe (without hose):
___ Other (explain):

c. Is there a building fire escape route:

(1) Describe type of emergency lighting in interior escape routes and power source:
(2) Describe alternate escape devices, e.g., ladders, rope, chute, etc:

d. List and describe all fires since last assessment:

9. Emergency communications

a. Type and Number of Radios:

(1) HF
(2) VHF/UHF
(3) Repeaters/Relays and Locations

b. Location of Base Station:

c. Number of residences with radios:

d. Number of agency vehicles with radios:

e. How often are communication checks conducted:

f. Who services radios:

g. List all staff and non-staff members who are issued radios:

10. Agency vehicles

a. List make, model, and year of each vehicle:

b. List any security modifications:

c. Number of official drivers:

d. Have they received driver training ?(if so, explain what):

11. Contract guard service

a. Name and Address of Contractor:

b. Effective date of contract:

c. Expiration date of contract:

d. Annual cost:

e. Name of Contractor Representative:

a
b
f. List each post and purpose:

g. Are guards armed and, if so, provide description of weapons:

h. Do guards have radios:

I. Who supplies and maintains guard equipment:

j. How do guards handle emergency notifications:

k. What role do they play in emergency situations, e.g., bomb threats, fires, etc:

a
b
l. Provide copy of contract and all special instructions:

12. Emergency procedures

a. Does the station have effective plans/procedures for:

___ Bomb Threats
___ Threatening Telephone Calls
___ Car-jacking
___ Hijacking
___ Kidnapping/Hostage Situation
___ Demonstrations and Protests
___ Natural Disasters

13. Local staff

a. Number of employees:

b. Number of contract hire employees:

c. What pre-employment checks are conducted for new employees:

14. Security training

a. Who is responsible for site security:

b. Is there a security briefing program for staff:

(1) Who provides the briefing:
(2) What does it address:

d. Are briefings for family members conducted:

(1) Who provides briefing:
(2) What does it address:

a
b
e. Describe security training programs available to/attended by staff members:
(e.g. mines awareness training)

Glossary of terms

Locks -

- primary
- auxiliary
- key-in-the-knob lock
- mortised locks
- deadbolt locks
- rim/surface mounted

Bibliography

Cutts M & Dingle A, 1995, *Safety first: protecting NGO employees who work in areas of conflict*, Save the Children, London

United Nations, 1995, *Security awareness, an aide-mémoire*, UNHCR, Geneva