USAID
FROM THE AMERICAN PEOPLE

Operational Security – General Information

An Additional Help for ADS Chapter 303

New Reference: 06/19/2006
Responsible Office: M/OAA/P
File Name: 303sae_061906_cd44

Operational Security – General Information

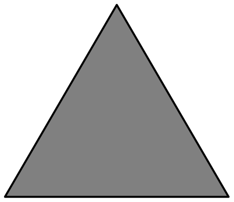
Operating in a Developing Country Context

This document raises a number of issues and provides general information regarding security. It is not prescriptive and does not seek to place any requirements on implementing partners. Additionally, every area/region presents its own specific and unique security challenges, so implementing partners must make their own determinations as to how to address such challenges. Therefore, implementing partners (i.e. contractors and recipients) should not interpret the information in this document as technical instructions, nor should they assume that the language herein constitutes a USAID position regarding the allow ability of certain security costs. This document will not be incorporated into any binding legal agreement between USAID and an implementing partner. When implementing any USAID award, the implementing partner bears the ultimate responsibility for ensuring adequate steps are taken to safeguard the security and safety of its personnel, and any USAID funded equipment/property/vehicles. The implementing partner is also responsible for ensuring that USAID funded equipment/property/vehicles are stored/maintained in accordance with applicable federal rules/regulations, as well as Mission-specific directives.

An intrinsic aspect of operating in a developing country is recognizing and addressing issues related to security. Most importantly, this includes the well-being of staff. The safety of personnel is a precondition for the activities of USAID and its implementing partners.

To achieve an adequate level of security, our contractors, non-governmental organizations (NGOs), and other implementing partners must see security as a top priority. It must be an integral component of program design and project management. Given the diversity of USAID's implementing partners, it is not possible to create a one-size-fits-all model. It is, however, essential for every organization to have both a well-defined concept of security as well as clearly articulated and consistently applied operational policies and procedures.

One of the most commonly used models, or analytical frameworks, for security consists of three axes: acceptance, deterrence, and protection:



Acceptance is the process of gaining widespread understanding and support for an organization's work on the part of local authorities, belligerents, and the population at large. This has been one of the fundamental principles under which civilian agencies have worked in conflict zones for many years. Acceptance depends in part on the articulation and adherence to humanitarian codes of conduct, such as impartiality. Acceptance has long been the foundation on which many non-governmental and international humanitarian organizations build their security approaches. While some would hold that undertaking humanitarian activities and building strong personal relationships accomplish acceptance, the process is more involved. Acceptance requires active outreach in the communities in which organizations conduct business, live, and implement programs. In short, outreach must extend to all parties with which an organization may come into contact – there should be no doubt about the identity of the organization or what it is doing.

It should be noted that a number of recognized experts in the field of humanitarian security suggest that acceptance has never been enough in and of itself, “everyone locks their doors.” Regardless of an organization’s view of this statement, each organization must be aware of the context in which it is working in order to determine the most appropriate approach to security and to what degree that approach includes or combines acceptance, protection, or deterrence strategies.

Protection encompasses the use of devices, such as physical barriers, armored vehicles, bullet-resistant vests, and satellite and two-way communications. It also includes procedures such as driving in convoys, varying routine, and the observance of curfews and "no-go" areas.

Deterrence is an approach whereby the threat is contained or deterred by the use of a counter threat. This could be legal, political, or economic sanction, but is most commonly an armed response.

In practice, most organizations use a combination of all three strategies. What's important is for an organization to make a conscience decision about where it wants to be inside the triangle, and to understand the advantages and drawbacks of this choice. Of note in that regard is the symbiotic relationship between organizations working in the same environment. For example, if one organization uses armed guards on convoys, others who do not may be more vulnerable.

Situational Awareness

It's clear that security begins with an appreciation of the environment in which one is operating. Nevertheless, it is frequently overlooked that what is safe in one place may actually increase risk in another. Whether to carry a weapon or stop after a vehicle accident depends on the nature of the threat and the specific situation. It is nearly impossible to create a list of hard and fast rules, which is why situational awareness is so critical. Effective situational awareness normally depends on team members developing accurate expectations for team performance by drawing on a common knowledge base –

a security plan. A security plan usually contains a policy statement, management responsibilities, procedural guidelines for prevention, guidance on radios and communications, evacuation procedures, checklists, and personnel contact numbers.

Threatening confrontations in the field can take many forms, including robbery, armed assault, vehicle hijack, crossfire, bombing, land mines, kidnapping and hostage taking. While some precautions can be taken to avoid such situations, even the most prepared field staff can become victims in a sudden confrontation. Therefore, advanced familiarity with the organization's principles and security plan will increase your staff's safety and chances for survival during a security incident.

An implementing partner may wish to designate a point person to handle these and other responsibilities related to security. This could be a senior position that reports directly to the Country Director or Chief of Party.

Information Sharing

Many organizations collect, analyze, and disseminate information on security. USAID's implementing partners may wish to establish and maintain regular contact with the Embassy Regional Security Officer (RSO) and other organizations, such as the Overseas Security Advisory Council (OSAC), United Nations groups (UNSECOORD, UNHCR, etc), and other larger umbrella groups operating in a country.

The sharing of information is often critical to situational awareness. For that reason, USAID suggests that each implementing partner report through the appropriate reporting organization all security incidents. In addition, any incidents involving death or injury to staff or which may materially affect the implementation of USAID-funded programs must be reported directly to USAID within 24 hours after the incident.

Field Travel

Most USAID implementing partners have the traditional structure of a headquarters office in the capital city and often sub-offices in the regions which implement programs in the field. Road accidents remain a major cause of injury and death for USAID workers and at least half of all security incidents occur during travel. Implementing partners may wish to establish and enforce procedural guidelines for field travel. Although the following list is not intended to be all-inclusive, an implementing partner might want to consider some of the following in generating its own guidelines:

- **Type of vehicle.** Choice of vehicle can impact on safety and security. Consider two- or four-wheel drive, choice of color, SUV/pickup or passenger vehicle, new or used, gasoline or diesel. New SUVs are the popular model for carjacks. The use of unmarked local or armored vehicles may be a better option in some cases.

- **Vehicle reliability.** Regularly scheduled maintenance and inspections should be conducted. Critical spare parts (e.g.: belts and hoses), consumables (oil, water, battery) and ancillary supplies (tools, tow rope, rations, first aid kit, spare fuel, etc.) should be carried at all times. Because armored vehicles have additional weight added on due to the armoring process, the vehicle is working harder than originally designed. Therefore, at a minimum, the normal manufacturers' maintenance cycle is half of what the manual reads (e.g. vehicle manufacturer recommends brake pads be replaced every 30,000 miles. In the case of an armored vehicle, USAID typically replaces its brake pads every 15,000 miles).

- **Number of vehicles and passengers.** A single vehicle and driver is a much easier target. USAID usually requires at least two people to ride in each of its vehicles, including one with language skills. Implementing partners might want to consider similar arrangements.

- **Day vs. night travel.** USAID does not recommend that its USAID staff drive at night, except in emergencies. Implementing partners might want to consider similar arrangements.

- **Cash in Transit.** The implementing partner might want to consider establishing procedures and guidelines for cash in transit. The implementing partner might consider varying travel parameters for each trip to the bank (time of day, day of week, route of travel, etc.) and consider the risks involved by combining bank runs with other errands.

- **Use of armed escorts.**

- **Use of bullet-resistant vests.**

- **Communications and GPS.** The implementing partner might want to consider both radio and satellite systems in each vehicle (see below), as well as a hand-held GPS unit.

- **Trip preparation.** The implementing partner might consider establishing a clear set of procedures be followed for planning the trip and notifying the appropriate parties beforehand. This may include checking the security situation, marking of primary and alternative routes, designating checkpoints/landmarks along the route to track the traveler's location, listing points of contact along the route, and estimating the approximate timeframe for the trip. Although it may not be necessary for short trips, the implementing partner might consider requiring that this information be put in writing and left with someone who will monitor the trip and be notified at its conclusion.

- **Emergency procedures.** These encompass a range of situations, from ambushes to landmines to checkpoints. The implementing partner might consider providing training or a detailed briefing to all drivers on standard procedures to follow in the event of an emergency.

Communications

Each implementing partner may wish to establish and maintain effective and reliable voice communications systems at all of its offices and with vehicles or personnel traveling in the field (including a back-up system). As appropriate, these systems may include HF and VHF/UHF radio systems and should include a minimum of one voice satellite system such as Thuraya, Inmarsat, or Iridium. Implementing partners might consider requiring that at least one system should not rely upon locally controlled infrastructure (e.g. cellular telephone systems).

Each implementing partner might want to consider the need to establish and maintain effective and reliable data communications at all of their offices. Discrete systems such as Vsat, Websat, or BGAN may be preferable, as well as a reliable source of power.

Each implementing partner should consider the wisdom of establishing and maintaining its own policies and procedures for the creation and maintenance of the following:

(1) Distributing and updating, at least monthly, a list of contact information for all internal and key external parties, including detailed information such as the location of staff housing and the tracking of staff on leave.

(2) A phone tree or warden system among the agency's staff that ensures all personnel can be contacted and accounted for in a timely manner.

(3) Training of staff on telephone and radio procedures and copies of frequencies/numbers and procedures available in offices and vehicles.

(4) Regular reporting or call-in procedures for staff living or traveling in the field.

Site Security

The goal of site selection and management is to establish, occupy, and maintain physical space(s) (residences, offices and warehouse) required to achieve operational objectives. The most effective site selection follows after a security assessment has been completed. Implementing partners might consider the following when selecting an office location:

- **Neighborhood** – level of crime, proximity to potential threats, known regions of adversarial activity, and politically or militarily significant buildings.

- **Accessibility** – single/multiple route access, road condition, ease of access or egress from the site, density of traffic, and accessibility of authorized and unauthorized vehicles.

- **Services** – water and electricity (including backup or portable generators).

- **Lighting** – to illuminate the site and surroundings, deter intruders, and aid observations.

- **Susceptibility to Hazards** – fire, floods, landslides, and winds.

- **Physical Space** – adequate for office, parked vehicles, storage, etc.

Based on the profile the implementing partner chooses to portray, and the dangers presented in any particular country situation, the following is a list of possible security applications. The list is not all-inclusive nor prescriptive; however, it provides general information on basic security applications that may help to improve the security posture of a facility.

- Construction of fencing or walls around the perimeter with alternate exit/entrances.

- Installation of perimeter barriers. Several types of temporary barriers, both passive and active, are available to mitigate vulnerability. To prevent bomb-laden vehicles from gaining access to a building's exterior, the implementing partner may wish to consider one of several types of barriers systems , including, but not limited to, the following:

    - Passive barriers provide anti-ram protection. They are stationary and may include planters, jersey barriers, bollards, earth berms, Hesco, Bastion revetment, and revetted trapezoidal ditches.
    - Active barriers provide anti-ram protection. These barriers move either side-to-side or up and down to allow vehicle entry and include hydraulic bollards, wedges, and sliding gates.

- For access control, installation of both passive and active barriers. For the exterior of a building, passive barriers may consist of razor wire, window grilles, steel plating, and other sustainable building materials. Active barriers may consist of turnstiles, security doors, and movable or hinged grille work.

- Protection of generators, water, and fuel. Heavy duty construction or the use of sandbags may be appropriate. The implementing partner may want to consider the wisdom of locating fuel supplies in the most remote area of the compound.

- Use of shatter resistant window film (SRWF) to all exterior and interior glass surfaces to reduce fragmentation of glass shards during a blast event. The implementing partner may wish to consult with USAID/SEC or the RSO for information concerning certified vendors.

- Installation of heavy-duty deadbolt locks near the top and bottom of a door to mitigate forced entry. To maximize the forced-entry protection, USAID normally installs deadbolt locks on either solid wooden or hollow steel doors.
- Installation of heavy duty forced-entry window grilles on all windows and/or man-passable openings as appropriate to mitigate civil disturbance and/or criminal

activity. **Fire Safety Note:** Window grilles are a fixed security application and careful consideration of fire egress should be considered. If a window requires movable or hinged grille work for fire egress purposes, the window grille will not be as effective for forced-entry protection. Fire protection, safety, and egress take priority over security. In most cases, both fire protection/safety and security can be achieved.

- Installation smoke detectors and security alarm system.

Implementing partners might consider the following when establishing their site security management:

- Testing smoke detectors and security alarm systems monthly.

- Maintaining a key rack and locked spare key box for facilities and vehicles, for easy access in case of an emergency. Strict control and accountability for keys is established.

- Ensuring that fire escape routes are known and fire extinguishers are charged and in correct locations and that staff know how to use the fire extinguishers.

- Ensuring that first aid kits are located strategically in the facility.

- Securing parking for vehicles. Street parking is normally discouraged.

- Establishing procedural boundaries – checkpoints, monitoring, and accountability for team member and visitor access.

- Closing and locking interior doors and windows when the office is empty, even for short periods of time. Establishing a daily office lock-up procedure with clearly defined staff responsibilities.

- Staggering lunch hours and breaks so that office is occupied during work hours.

- Hiring guards for both office and parking area, if needed.

- Informing all staff members of security measures and procedures including:
    - 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
- Providing the location and purpose of safe havens.

- Furnishing bomb and bomb threat procedures.

Emergency/Evacuation Plans

Implementing partners might want to consider developing a plan to guide their actions in the event of an emergency. Any such plan might consider a rapid, forced withdrawal from an area of high risk and the temporary suspension of activities. Such a plan might also include some of the following:

- Tracking of security phases/operational alert levels (green, yellow, red, etc.).
- Coordination with USAID, other donors, and appropriate embassies.
- Shutdown procedures, including the collection or destruction of sensitive materials and equipment.
- Designation of assembly points.
- Stockpiling of survival equipment and supplies (amount, location, access).
- Transportation methods and designated POCs for evacuation (road, air, water).
- Evacuation points and routes (airport, border, specific road, etc.) marked on maps.
- Preparation of vehicles.
- Rehearsal and refinement of the plan on a regular basis.

The need for additional plans and planning is area or program specific, i.e. plans developed for one area or organization will most likely be ineffective in/for another.

Additional Resources and Information

The Overseas Security Advisory Council (OSAC), the Embassy Regional Security Officer (RSO), USAID's Office of Security, the United Nations Minimum Operating Security Standards (UNMOSS), RedR, Geneva Centre for Security Policy (GCSP), and Humanitarian Practice Network's (HPN) Good Practice Review "Operational Security Management in Violent Areas" are all excellent resources in security planning and management.

Final Note

The aspects of security outlined above are listed in order of importance and difficulty. Situational awareness is undoubtedly the hardest to accomplish, but it is also the most critical to good security. Many organizations hire a security consultant to make such recommendations as the required security countermeasures, security guidelines, evacuation plan, etc. A security plan should be kept current.

In most cases, the organization’s senior leader has the overall responsibility to monitor and relay safety and security issues to those in his or her group. Being aware of personal and team safety and security is the responsibility of every group member. USAID and the State Department's Regional Security Office may be seen as a resource for developing effective countermeasures. Specific questions and comments may be directed to your Cognizant Technical Officer. He/she may then refer you to an appropriate party.