

**Mandatory Reference:** N/A  
**Supplementary Reference:** 562  
**File:** adscd15/56253s1

## **OVERSEAS SECURITY PROCEDURES GUIDE**

### Forward

The following serves as a guide to assist Unit Security Officers in the formulation and implementation of standard operating procedures. The guide is designed to cover a wide spectrum of USAID security-related operations. Users are encouraged to use, modify or expand on those sections that pertain to their specific needs. The language suggested in this guide is for illustrative purposes only. Procedures developed based on this guide must be coordinated with the RSO.

# OVERSEAS SECURITY PROCEDURES GUIDE

## CONTENTS

### I. NORMAL CONDITIONS

#### A. Duty Hour Procedures

1. Routine Duties
2. Personnel Identification
3. Vehicle Identification and Parking
4. Personnel Screening
5. Vehicle Inspection
6. Visitors/Escorts
7. Public Access Controls
8. Char Force

#### B. After-hours Procedures

1. General
2. Access Control
3. Inspections
4. Night Time Guard Duties

### II. EMERGENCY CONDITIONS

#### A. Hostile Activities (Terrorist or Mob Attack)

1. Advance Notification
2. General Notification
3. Emergency Lock-up
4. Assembly/Accounting for Personnel
5. Warden System
6. Safe Haven

#### B. Fire

1. Notification
2. Evacuation Procedures
3. Host Government Responsibilities

#### C. Bomb

1. Telephonic Bomb Threat
2. Notification

- 3. Evacuation Procedures
- 4. Host Government Responsibilities

### III. RECEPTIONIST

- A. ROUTINE DUTIES
- B. EMERGENCY DUTIES
  - 1. Telephonic bomb threat procedures.
  - 2. Terrorist or mob attack procedures.
  - 3. Fire procedures.

### IV. UNIT SECURITY OFFICER EMERGENCY DUTIES

## PROCEDURES

### I. NORMAL CONDITIONS

#### A. DUTY HOUR PROCEDURES

1. ROUTINE DUTIES - The following is a general guideline that provides a basic description of Guard and Receptionist duties:

##### a. Public Access Control (PAC) Lobby Guard

(1) The PAC Lobby Guard provides stationary guard coverage outside of the PAC hardline at the main entrance to the USAID. The Guard is expected to resist attack and serves as the first line of defense against harm to USAID personnel.

(2) The PAC Lobby Guard performs access control and visitor screening functions as follows:

(a) Examines visitor packages for weapons, contraband and explosives;

(b) Conducts metal detector checks of visitors for weapons and explosive devices;

(c) Logs visitors and issues visitor badges;

(d) Verifies identification;

(e) Facilitates visitor escort procedures; and

(f) Ensures that packages of unknown content have not been left in the lobby.

##### b. Receptionist

(1) The receptionist is normally located behind the PAC hardline in a security booth. The receptionist verifies identification and points of contact for all visitors. The PAC lobby guard notifies the receptionist that the visitor will or will not be permitted access. If entry is authorized, the visitor shall require an escort (USAID staff employee). Entry is not permitted until the escort arrives.

(2) The receptionist conducts periodic checks and tests of

the security systems when authorized by the USAID Executive Officer. As a minimum, these include a check of: the security door control system (working status of switches and indicator lights); security door emergency locks; alarm system; and telephone and/or other communications equipment at the security station (booth).

(3) The receptionist maintains awareness of activity in the lobby to ensure unauthorized persons do not gain entry into USAID office areas; and ensures that the PAC lobby guard is not under duress.

2. PERSONNEL IDENTIFICATION - All persons requiring access to the USAID compound/facility must have valid identification such as an:

- a. American Embassy issued ID card;
- b. USAID issued ID card;
- c. State Department Building Pass; or a
- d. U.S. Diplomatic Passport.

3. VEHICLE IDENTIFICATION, INSPECTION, AND PARKING -

- a. Vehicles authorized to enter the USAID compound are identified as those with diplomatic license plates (or describe license plates or other identifying information for those vehicles authorized access or parking on the USAID compound).
- b. Vehicles not authorized compound access are denied access to the facility. Authorized visitor vehicles are directed to appropriate parking areas. Visitor parking shall not be permitted within 50 feet of the USAID main office building.
- c. All vehicles entering the USAID compound are subject to inspection to prevent introduction of dangerous devices or weapons. Vehicle inspections are conducted at the point of entry by the assigned guard force.
- d. The local guard force is directed to physically inspect the under carriage, under the hood (engine compartment), the trunk (luggage compartment), and to view the vehicle interior, noting any suspicious items. If a suspicious object/item is detected, the guard shall require the occupant(s) to further identify the item.

e. Upon detection of a suspect item, the vehicle is not permitted to proceed any further. The senior guard supervisor, USAID Executive Officer, and RSO shall be notified immediately if vehicle entry is denied.

f. Procedures affected upon detection of an explosive or other dangerous devices. (This section is to be developed and coordinated with the RSO), based on local conditions and "render safe" capabilities of the host country. Movement of the suspect vehicle away from the compound must be considered as a further risk. Evacuation of personnel from the building or compound must also be considered.)

4. PERSONNEL SCREENING - All visitors requiring entrance to the USAID compound/facility are subject to metal detection screening. All packages, parcels, bags, and briefcases are subject to inspection prior to entry onto the USAID property. The screening shall be accomplished at the main entrance by the assigned guard force.

5. VISITORS/ESCORTS - Visitors to the USAID facility shall be treated in a courteous and polite manner at all times. The following procedures are to be followed for visitor access to the USAID compound:

a. After a visitor has made a request to the local guard for access to the USAID facility, the guard shall phone the party being visited and inform them of the visitor's presence. The office/person being visited must authorize access for the visitor. The office/person being visited shall be responsible for escorting the visitor to and from the point of entry.

b. Visitor escort is the responsibility of the office/person being visited. The objective is to expedite the visitors entrance to the proper office in an efficient manner. This will prevent persons from wandering about and provides a modicum of decorum and respect for the visitors.

6. PUBLIC ACCESS CONTROLS (PAC) - Under the supervision of the RSO and the USAID USO, the PAC system is operated by the local guard force or receptionist in accordance with these procedures and local guard orders. The PAC system employs door control consoles and electronic locking devices. Security door components are briefly described below.

a. Panic Exit Devices (Crash Bars) - These items are used in conjunction with electric release strikes and may be operated by cipher/combination simplex during normal working hours. The devices are not to be left in the open or unlocked position.

b. Combination Cipher Locks - These devices are used during normal working hours in conjunction with the panic devices. The combinations may be given to all employees having a need for access to the offices. Combinations shall be denied to others not having a valid need for access. They are not intended to be, nor are they considered ultimate security devices for after-hours use (see item d.).

c. Forced Entry Locks - These locks are located at the top and bottom of each security door. The forced entry locks must be manually engaged in order to provide forced-entry resistance in the event of an emergency. USAID personnel located in the general area of the security doors should be assigned the responsibility to insure manual engagement of the locks in an emergency situation. The USO must verify that the locks are correctly engaged during an emergency. The locks are normally left in the open position and should not be used for normal lockup.

d. Dead Bolt - Each security door is equipped with a manual dead bolt, located in the central area of the door. This manual lock is to be used for night time lockup.

e. Electromagnetic Emergency Locks (Entrances) - These locks are located at the top of the door and are designed to provide immediate lock-up capability in the event of an emergency. This is intended solely to give personnel time to engage the forced entry locks (previously discussed). Except during emergencies, the magnetic locks on entrance doors are not engaged at any time.

f. Electromagnetic Locks (MAGLOCKS)- The MAGLOCKS locks on doors designated as emergency exits must be engaged at all times. During normal working hours, the forced-entry locks must remain unlocked at all times to facilitate emergency egress due to fire or other emergencies. The door is equipped with a Request to Exit push bar that will interrupt the electrical power and disable the MAGLOCK when it is pushed. An alarm annunciator will sound when the door is opened and can only be reset with a key maintained by the USO. The alarm also serves to aid personnel in locating an emergency exit during a fire or other emergency. A sensor will also alert the receptionist that the door has been opened. The MAGLOCK will relock when the door is closed.

7. CHAR FORCE - USAID offices are usually cleaned by an unescorted char force during normal working hours. An escort during normal working hours is not necessary, but it is the responsibility of all employees to note

any unusual activities conducted by the char force and report same.

## B. AFTER-HOURS PROCEDURES

### 1. GENERAL

- a. Main entrance security doors shall be locked (the center dead bolt engaged) after hours. The cipher lock system is only for day-time use. All other areas shall be locked in accordance with existing directives.
- b. All keys are to be secured in accordance with procedures established by the USO. Persons having building keys are responsible for maintaining control of the keys at all times. A spare set of building keys must be stored in the Embassy at all times under the RSO's control.
- c. Local personnel, foreign service nationals (FSNs) or guards, shall not occupy the primary building after normal working hours. Exceptions to this requirement must be cleared and approved by the RSO.

### 2. ACCESS CONTROL

- a. Only authorized USDH personnel will be allowed access to the compound during non-duty hours. FSNs and other personnel requiring access to the compound after hours must obtain prior approval from the USO and have written authorization from their USDH supervisor.
- b. Non-regular employees, contractors, and visitors must be escorted by USDH personnel after normal working hours.
- c. Only authorized USDH and FSN personnel (with prior approval of the USO) shall be allowed to receive keys for access of USAID buildings.
- d. An after-hours log shall be maintained at the main entrance for all personnel working after normal hours (weekends and holidays included) to log in and out.

3. INSPECTIONS - The USO shall conduct periodic after-hours inspections of the USAID premises. These inspections are to ensure that classified and/or controlled information is properly secured or returned to the Embassy for storage. The inspections also serve to ensure that the building is properly locked and electrical appliances are turned off.



4. NIGHT TIME GUARD DUTIES - Written guard orders are provided to the guard supervisor by the USO. A review of the guard orders should be conducted periodically to update the orders as necessary. The RSO should be consulted for guidance in this matter. The guard orders should be brief, but specific, and cover the following items:

- a. Patrolling the compound;
- b. Occupancy of the building after hours;
- c. After-hours and weekend log;
- d. Compound lights; and
- e. Police/assistance procedures.

## II. EMERGENCY CONDITIONS

### A. HOSTILE ACTIVITIES (TERRORIST OR MOB ATTACK)

1. ADVANCE NOTIFICATION - Occasionally, information becomes available that advises U.S. authorities that a demonstration, mob action, or an organized attack is being orchestrated against specific U.S. facilities. Upon being notified of an imminent action directed against the USAID facility, all personnel shall be alerted accordingly. This is accomplished as follows:

- a. Silent - In some instances word of mouth or telephone calls may be more efficient and less likely to cause panic. This is to be determined locally, dependent on the circumstances.
- b. Audible - Using the appropriate alarm of the alert system (Selectone) and voice capability is the fastest and surest method to notify all personnel located in the compound of immediate danger. It is essential that personnel become familiar with the meanings of the various Selectone signals. Routine testing is critical.

2. GENERAL NOTIFICATION - If advance information is not available, the guard force will be the logical first point of contact for detecting any hostile intent by a mob or attacking force. The receptionist will normally be responsible for giving notification via the alert system (Selectone). (Guard orders are to be written to clearly advise when to activate the alert system.)

3. EMERGENCY LOCK-UP - Upon being alerted to an emergency

situation, the guard force/receptionist will immediately initiate emergency lock-up procedures. The first step is to activate all of the magnetic locks via the door control console. (Guard orders shall be written to clearly advise when to initiate the lock-up system.)

#### 4. ASSEMBLY/ACCOUNTING FOR PERSONNEL

- a. In the event emergency procedures are activated, the senior USAID officer present shall advise the U.S. Embassy of the situation and request assistance if required. The focal point is the RSO or the Marine Security Guard (MSG). This may be accomplished via radio or telephone.
- b. Personnel not in the USAID facility at the time of an emergency shall make every effort to contact the USAID or the Embassy for further instructions. Personnel will not gather at the USAID compound unless so directed.
- c. The senior USAID officer present shall account for all personnel as soon as practicable, to determine who is missing and where other personnel may be located. Efforts shall be made to contact personnel unaccounted for via radio.

5. WARDEN SYSTEM - USDH personnel are assigned duties as building wardens in the event of an emergency. An alternate building warden is also assigned in case of absence of the primary warden. The following are duties and responsibilities:

- a. Ensure that all personnel are notified and follow all emergency instructions;
- b. Ensure forced-entry manual locks on all entrance and exit doors are engaged;
- c. Other duties as may be assigned by the USO.

6. SAFE HAVEN - Upon notification of an emergency situation, steps must be taken to provide protection for personnel. This shall be in accordance with the Emergency Action Plan (EAP) established for the U.S. Diplomatic Mission. This may be the disbursement of personnel (send personnel home or away from the anticipated attack zone) or by taking refuge in the designated safehaven or safe area. The following procedures apply:

- a. Once personnel are in the designated safe area, the security doors shall be locked using the forced entry locks and the night

time dead bolt.

b. The emergency exit is kept clear and all manual locks are engaged.

c. A radio with U.S. Embassy emergency and evacuation (E&E) frequency shall be present in the safe haven and connected to an external antenna. A standard portable antenna shall also be available in case the external unit is damaged or destroyed. If affixing a permanent radio in the safe haven is not feasible, the USO shall be responsible for insuring that a radio is available for this purpose.

d. Each safe haven/safe area shall be equipped with minimum emergency supplies. These supplies typically consist of food (i.e., military rations), potable water, portable sanitary waste system, blankets, first aid kit, or other items deemed necessary by the USAID. Safehaven kits are available from Bureau of Diplomatic Security. USOs may request them via the RSO.

B. FIRE: All classified information shall be secure. All guidance relating to actions in event of fire shall be obtained from the safety officer.

### C. BOMB

1. TELEPHONIC BOMB THREAT - Persons receiving a telephonic bomb threat shall obtain as much information as possible from the caller. Other information, such as background noises, regional accents, etc, are also to be noted. Upon receipt of a bomb threat call, the USAID employee shall immediately notify the USO, EXO, senior USAID official, and the RSO or Post Security Officer (PSO) (specific actions are to be prescribed by the USO).

2. NOTIFICATION - Personnel detecting a suspicious package, bag, brief case or other type of container suspected of containing an explosive device shall immediately notify the entrance guard/receptionist and the Executive Office for determination of appropriate action. **IN NO INSTANCE ARE PERSONNEL TO MOVE, TOUCH, OR OTHERWISE DISTURB THE DEVICE!**

3. EVACUATION PROCEDURES - Personnel shall evacuate the building or area in accordance with the published Bomb Evacuation Plan as established by the EXO in consultation with the RSO.

4. HOST GOVERNMENT RESPONSIBILITIES - The RSO must be notified immediately of any suspicious item. The RSO will then take

appropriate action and provide liaison with the host government authorities regarding disposal of the suspect device.

### III. RECEPTIONIST EMERGENCY DUTIES

A. TELEPHONIC BOMB THREAT PROCEDURES - The receptionist obtains appropriate information about the threat, caller, and background sounds (post-provided bomb threat forms should be used). Upon receipt of notification of threat from other employees notifies USO, senior USAID official, and or RSO/PSO (specific procedure as prescribed by USO); and activates bomb threat alarm as directed.

B. TERRORIST OR MOB ATTACK PROCEDURES - The receptionist activates all security door emergency locks; activates terrorist attack alarm; notifies USO, senior USAID official, RSO/PSO and host government police/military forces (specific procedure as prescribed by USO and contained in instructions); activates forced entry locks on those security doors under responsibility of the receptionist.

C. FIRE PROCEDURES - The receptionist announces the nature of fire threat via microphone and activates fire alarm; deactivates any engaged security door emergency locks; calls fire department; vacates room and removes any emergency radio equipment.

### IV. UNIT SECURITY OFFICER EMERGENCY DUTIES

In an emergency, to include evacuation of the USAID, the USO is responsible for ensuring that all classified information is secured in a proper container, removed to a safe location or destroyed as required by the RSO or the Emergency Action Plan.