
# ADS Chapter 562

# Physical Security Programs (Overseas)

Partial Revision Date: 11/22/2019
Responsible Office: SEC/ISP
File Name: 562_112219

**Functional Series 500 – Management Services**
**ADS 562 – Physical Security Programs (Overseas)**
**POC for ADS 562: David Blackshaw, (202) 712-1259, dblackshaw@usaid.gov**

## Table of Contents

# ADS 562 - Physical Security Programs (Overseas)

## 562.1 OVERVIEW

Effective Date: 07/01/2006

This chapter identifies the overseas physical security policy directives and required procedures for the protection of USAID employees, facilities, classified national security, and Sensitive But Unclassified (SBU) information.

## 562.2 PRIMARY RESPONSIBILITIES

Effective Date: 11/22/2019

**a.** The **Office of the Administrator (A/AID) staff** notifies the Office of Security, Division of International Security Programs (SEC/ISP) well in advance of any overseas travel by the USAID Administrator (A/AID) or Deputy Administrator (DA/AID) (see **562.3.10**).

**b.** The **Office of Security (SEC)** has primary responsibility for interpreting, supplementing, and developing physical and technical security policy directives, required procedures, and for oversight of physical and technical security enhancements for USAID offices.

**c.** **Bureaus/Independent Offices (B/IOs) and Missions** are responsible for notifying SEC prior to any action that will affect the existing use of USAID office space.

**d.** **USAID Senior Managers (Assistant Administrators, Mission Directors, USAID Representatives, and Office Directors)** are directly responsible for ensuring that all employees and contractors under their authority understand and follow the USAID security policy directives and required procedures contained in this ADS chapter.

**e.** **USAID Executive Officers (EXOs)** coordinate and monitor security operations and physical/technical security systems within their respective Mission.

**f.** **USAID employees and contractors** are responsible for complying with USAID security policy directives and required procedures as reflected in this ADS chapter.

**g.** **Regional Security Officers (RSOs)** are responsible for the operation of all security programs and protection functions at overseas posts.

**h.** The **Bureau for Management, Office of Management Services, Overseas Management Division (M/MS/OMD)** is responsible for approving the lease or purchase of USAID overseas office space.

## 562.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

### 562.3.1 Overseas Office Building Security

Effective Date: 11/22/2019

**a.** B/IOs and Missions must notify SEC in writing of any potential action that may affect the use of office space, such as:

- USAID openings, closings, relocations, or adding additional office space outside the established hardline;
- Staff increases or decreases;
- Other activities necessitating changes in the physical security provisions for office space;
- Any temporary lease of space for meetings, conferences, swing space, or surge capacity requirements; and
- The proposed receipt, storage, processing, or discussion of classified national security information.

B/IOs and Missions must notify SEC with regard to the above-listed circumstances as far in advance as possible, regardless of the location, duration, and number of employees involved.

**b.** Classified national security information: Must not be received, stored, processed, or discussed at a Mission outside a controlled access area (CAA). Missions initiating a proposal to receive, store, process, or discuss classified national security information must cable the request to SEC for clearance and ultimate delivery of the proposal to the State Department's Bureau of Diplomatic Security (DS). A post must demonstrate to SEC and DS a legitimate need to have material at a given location, as well as provide a justification for the level of classified information to be stored. Prior to final approval, either DS and/or SEC must conduct a site survey. Both SEC and DS must approve this survey prior to implementation of any classified operations.

**c.** Leases: USAID B/IOs and Missions must not sign any lease to acquire additional office space in existing facilities, relocate to new office buildings, construct new office buildings, or acquire any other type of functional space without the prior written approval of SEC. This requirement is in addition to the Bureau for Management, Office of Management Services, Overseas Management Division (M/MS/OMD) approval required by **15 FAM 312**. Prior to lease approval by M/MS/OMD, SEC must ensure that a security assessment is

performed to determine whether the facility can meet the minimum-security standards described in **12 FAH-5**, **12 FAH-6**, and **12 FAH-11**. (Note: These links are classified and/or are only available through ClassNet. For information on these documents, please contact Nancy Aposporos, **naposporos@usaid.gov**).

**d.** Physical and technical security systems: SEC designs and installs physical and technical security systems in consultation with USAID Mission Management, the Regional Security Officer (RSO), Security Engineer Officer (SEO), Information Management Officer (IMO), and other appropriate offices in USAID/Washington.

### 562.3.2 Physical and Technical Security Standards

Effective Date: 11/22/2019

**a.** New office buildings (NOBs), newly acquired buildings (NABs), and other functional space, whether acquired by purchase, long-term lease, or short-term lease, must meet all physical and technical security standards contained in this ADS chapter and Department of State (DOS) standards **12 FAH-5**, **12 FAH-6**, and **12 FAH-11**, unless otherwise specified therein. This policy applies to standalone facilities, commercial office space, embassy/consulate buildings, and annexes. Missions must not occupy new facilities until SEC grants them written approval.

**b.** SEC has modified the standards in **12 FAH-5**, **12 FAH-11** and **12 FAH-6** for USAID as follows:

- In all situations where **12 FAH-6** calls for compound access control (CAC), walls of the remaining portions of the CAC will be constructed of some substantial material, *i.e.,* concrete masonry units or "cinder block," masonry, brick or concrete. All non-forced-entry/ballistic resistant (FE/BR) windows and door glazing on the street side will be grilled and provided with an application of eight mil (0.2 mm) of performance equivalent shatter-resistant window film to the interior side, or with laminated glass (12 mm thick) in a steel frame with 25 mm bite, the 15-minute forced entry and ballistic resistant (FE/BR) standard must be used.

- In all situations where **12 FAH-11** calls for safe haven technical security systems to be installed, USAID will use the Security Engineering Branch configured safe haven cabinet configuration.

- When feasible, USAID office buildings will incorporate a public access control (PAC) man-trap as part of the hardline.

- When feasible, USAID office buildings will incorporate a Security Management System enterprise (SMSe) that is directly connected to the U.S. Embassy SMSe infrastructure.

- All active anti-ram wedge barriers must have the Dragon Teeth modification applied.

- FE/BR doors on all USAID office buildings, compound access control (CAC) guard booths/pedestrian screening areas, and Safe Area or Safe Haven generator rooms must have M-3 Medico lock cores.

- In all situations where **12 FAH-5** calls for a five-minute forced entry standard for doors, the 15-minute forced entry and ballistic resistant (FE/BR) standard must be used.

- In all situations where **12 FAH-5** calls for a five-minute forced entry standard for window grilles, the 15-minute FE standard must be used.

- All newly acquired USAID office space that includes more than one floor, or multiple sections of one floor of a building, must be contiguous.

- USAID must not occupy more than 25 percent of the square footage of a commercial office building. In no case must the total United States Government (USG) staff, including Foreign Service National (FSN) employees, exceed 50 percent of the total building staff population.

- USAID Safe Areas and Safe Havens must accommodate a minimum of 50 percent of the USAID staff and be designed for a minimum of ten square feet per person.

- Alteration, removal, disabling, modification, or movement of USAID security systems and components is not authorized without the written concurrence of the Regional Security Officer (RSO) and written approval of SEC. Security systems and components include, but are not limited to, inspection/screening areas, public access control area doors and windows, emergency exit doors, locking hardware, audio alarm systems, closed circuit TV systems, security communication equipment, X-ray, explosive detection, and metal and package screening devices.

### 562.3.3 Exception Requests

Effective Date: 11/22/2019

**a.** Requests for exceptions to physical security standards must be handled in accordance with the policy directives and required procedures outlined in this chapter and **12 FAH-5 H-200**.

**b.** B/IOs and Missions must request exception(s) when Overseas Security Policy Board (OSPB) standard(s), outlined in the 12 FAH-6, cannot be met. A waiver(s) must be requested when a statute(s) contained in the **Secure Embassy**

**Construction and Counter-Terrorism Act (SECCA) of 1999 (P.L. 106-113)** cannot be met.

There are two statutory security requirements of SECCA of 1999 – P.L. 106-113:

1. In general, Section 606 (A)(2) provides that the State Department, in selecting a site for any new U.S. Diplomatic Facility abroad, must collocate all U.S. Government personnel at the post (except those under the command of an Area Military Commander) on the site. In effect, this makes the existing security policy set forth in **12 FAH-5** statutory.

2. In general, Section 606 (A)(3) provides that each newly acquired U.S. Diplomatic Facility must be situated not less than 100 feet from the perimeter of the property on which the facility is to be situated.

Missions must request a Regional Operational Officer (ROO) to conduct an assessment of the proposed facilities. SEC encourages a joint visit by M/MS/OMD to ensure a comprehensive assessment is performed. Post will be required to support the ROO and M/MS/OMD team by providing the below:

- Identification of the specific standard(s) to be waived;
- Justification for the exception;
- Statement of Agency operational requirements;
- Permits;
- Site plan, maps, and photographs;
- Floor plan (Building Plans);
- Description of the building;
- Description of existing security measures; and
- Chief of Mission (COM) and RSO comments and recommendations.

**c.** SEC will evaluate the package to ensure that the physical/technical security viability is complete. Next, SEC will forward the evaluation to M/MS/OMD and the applicable B/IO for comments before sending it to the Administrator for approval/disapproval prior to forwarding to Department of State's Diplomatic Security (DS) for a final decision.

### 562.3.4 USAID Internal Security Procedures
Effective Date: 11/22/2019

**a.** EXOs must take an active role in the security procedures and functioning of security equipment at USAID owned facilities, (*i.e.,* standalone compounds, tenant of commercial office space, and annexes). The EXO must immediately report to the RSO and SEC any discrepancies of security procedures or equipment.

**b.** EXOs are responsible for ensuring the proper preventive maintenance on all security equipment issued and/or installed by SEC at a Mission.

### 562.3.5 Overseas Security Budget and Funding
Effective Date: 11/22/2019

Overseas security budget and funding must be handled as follows:

- Missions are responsible for funding the maintenance cost of the physical and technical security systems, which includes Mission armored vehicles, active anti-ram barriers, compound access vehicle/pedestrian gates, security battery replacement, and shatter resistant window film.
- SEC will fund the repair, replacement, and lifecycle of physical and technical security systems as needed.
- Missions must absorb all security project costs when they relocate or acquire additional office or other functional space that was not approved in advance by M/MS/OMD, the respective geographic B/IO, and SEC.
- Missions are responsible for funding all unprogrammed residential security costs that may evolve from increased personnel staffing.
- Missions and RSOs are responsible for funding host government facilities occupied by USAID staff.

### 562.3.6 Overseas Residential Security and Local Guard Programs
Effective Date: 07/01/2006

The Department of State administers the Overseas Residential Security and Local Guard Programs through the RSO at post. Refer to **12 FAH-6**, which is maintained by the RSO. USAID participation in these programs is in accordance with these policy directives and required procedures:

- Prior to leasing or purchasing a residence, the EXO must obtain RSO approval to ensure that security-related issues are addressed during the selection of prospective residences.

- When security standards are not met, the EXO must document security needs and request residential security upgrades and/or funding assistance from the RSO for U.S. Direct-Hire (USDH) residences (see **562.3.7** for funding restrictions).

- Where the RSO cannot provide security upgrades and/or funding, for USDH residences, Missions may request funding assistance from SEC. Such requests must be accompanied by an RSO statement showing that Department of State funds are not available.

- All requests SEC funding assistance and SEC overseas security services must be requested via cable to SEC.

### 562.3.7 Department of State Residential Security Program Funding Restrictions

Effective Date: 11/22/2019

**a.** Department of State funding for the residential security program applies only to USDH employees. All residential security equipment requirements for U.S. contractors (long-term Personnel Services Contractors (PSC) or contractors funded through program funds) must be funded through the applicable contract.

**b.** Missions must establish a parallel residential security program for U.S. citizen contractors. Missions must coordinate with the RSO to determine the costs for the purchase and installation of the requisite equipment for contractor personnel and arrange funds accordingly.

### 562.3.8 Security Equipment Accountability, Control, and Maintenance

Effective Date: 11/22/2019

**a.** Record Keeping: Missions must record all physical/technical security equipment in the approved inventory systems at post. SEC maintains ownership of all physical/technical security equipment to include the approval for disposal, in accordance with the provisions of **14 FAM 410** and **ADS 534, Personal Property Management Overseas**.

**b.** Accountability:

- Missions are accountable for all SEC-funded security equipment. This equipment is considered non-expendable property (NXP), with the exception of certain low-dollar-value, non-serialized items, such as mechanical locks;

- Missions must enter all NXP security equipment into the USAID property account or inventory logistics management system (ILMS), regardless of

the funding source or whether used by Direct-Hire employees or contractors. In case of a staff reduction or USAID closure, SEC will provide disposition instructions; and

- Missions must provide copies of property survey reports for lost and stolen security equipment to SEC.

**c.** Maintenance:

The EXO must ensure that all physical/technical security systems receive preventive maintenance. The EXO must:

- Notify the RSO and SEC/International Security Programs (ISP) when maintenance needs are beyond the capabilities of the USAID or RSO staff,

- Submit a work request in the computerized maintenance management system (CMMS) on all deficiencies relating to physical/technical security systems, and

- Contact SEC for assistance, in the event that the RSO cannot provide assistance within a reasonable period of time.

### 562.3.9 Locks, Keys, and Combination Controls

Effective Date: 11/22/2019

**a.** Locks, keys, and combination controls within USAID:

RSO and SEC approval is required prior to the installation, modification, or removal of any security locking devices used for the protection of a control access area (CAA), limited access area (LAA), FE/BR hardline doors, and FE/BR exterior office space doors in any USAID facility.

For Missions that are authorized classified operations or Missions that are unclassified and both without 24-hour guard force coverage, refer to **12 FAM 446, Building Security - Lock and Leave (L&L) Policy**.

**b.** Keys: Mission Directors must appoint principal and alternate Key Custodians to manage the Key Watcher system. The appointees must be cleared U.S. citizens.

**1)** The Key Custodian will manage the upkeep of the Key Watcher database and will issue key dates and times in accordance with the EXO guidance. Security keys can include but are not limited to: FE/BR doors, CAA spaces, LAA spaces, Server/Telecoms rooms, Safe Area/Haven generator rooms, cashier rooms, armored vehicles, and any other sensitive area that requires key control.

**2)** SEC's Security Engineering Branch is the only authorized office to pin lock cores and cut keys on security locking devices for Missions.

**c.** Combinations: The combinations on all security equipment must be changed under the same criteria used for combinations on security containers as stipulated in **ADS 568.3.3.2**. The Unit Security Officer must maintain a central record of all combinations within the Mission, and must ensure that the RSO has a copy of the up-to-date central record.

## 562.3.10 Security of the Administrator during Travel

Effective Date: 11/22/2019

**a.** The Office of Security, International Security Programs Division (SEC/ISP) is the only office authorized to coordinate the personal protection of the USAID Administrator, Deputy Administrator, and other employees designated by the Administrator during travel to critical and high-threat posts.

**b.** A/AID staff must notify SEC by memorandum in advance of the proposed travel. This memorandum must list the senior participants, proposed itinerary, and trip objectives.

**c.** SEC provides recommendations about security requirements and coordinates with appropriate entities in State/DS and Post Management to supply protective escorts, security guidance, and individual briefings.

**d.** When deemed necessary, SEC must obtain protective escort services from the Bureau of Diplomatic Security on a reimbursable basis.

## 562.3.11 Terrorist and Criminal Incident Reporting

Effective Date: 11/22/2019

**a.** The EXO or Mission Director designee must report to SEC and the State Operations Center all terrorist and criminal incidents affecting USAID employees, contractors, their dependents (overseas), and implementing partners after notifying the appropriate local RSO. USAID staff, who become aware of security incidents involving implementing partners, must also report these incidents to SEC.

**b.** When a serious incident occurs, Missions must immediately telephone the State Operations Center which will in turn contact the USAID/W Duty Officer. The USAID/W Duty Officer will notify the SEC Duty Officer. The Mission must forward a follow-up telegram to SEC within one workday after the incident. The Mission must follow the requirements for handling classified information at all times (see **ADS 568, National Security Information Program**).

A serious incident may include, but is not limited to, those which affect the operational status of USAID, such as:

**1)** The USAID office building has been attacked or sustained damage due to bombing, mob violence, or terrorist assault;

**2)** USAID personnel have been taken hostage, injured, or killed in other than accidental circumstances; and

**3)** USAID facilities, residences, or personnel are under imminent threat of attack.

**c.** At overseas Missions, reports by telephone, telegram, and email must include the following:

- A summary of the incident;
- Date and local time that the incident occurred;
- Location of affected facilities;
- Type of incident;
- Number, identification, and affiliation of personnel affected by the incident;
- Effect of the incident on USAID operations;
- Identification of damaged equipment;
- Estimated cost and time to repair/replace the equipment;
- Response of host government forces; and
- Security countermeasures implemented.

Note: Reporting incidents may contain sensitive or even classified information and therefore any report must be cleared through the proper channels at post.

## 562.4 MANDATORY REFERENCES

### 562.4.1 External Mandatory References

Effective Date: 11/22/2019

**a.** **12 FAH-5, Department of State, Physical Security Handbook**

**b.** **12 FAH-6, Department of State, OSPB Security Standards and Policy**

**Handbook (Classified)**

**c.** **12 FAH-11, Technical Security Systems Handbook (Classified)**

**d.** **12 FAM 446, Building Security - Lock and Leave (L&L) Policy**

**e.** **14 FAM 410, Personal Property Management for Posts Abroad**

**f.** **15 FAM 312, Leasing Policy**

**g.** **Secure Embassy Construction and Counter-Terrorism Act (SECCA) of 1999 (P.L. 106-113)**

### 562.4.2 Internal Mandatory References

Effective Date: 09/28/2005

**a.** **ADS 534, Personal Property Management Overseas**

**b.** **ADS 561, Security Responsibilities**

**c.** **ADS 568, National Security Information Program**

## 562.5 ADDITIONAL HELP

Effective Date: 11/22/2019

There are no additional help documents for this chapter.

## 562.6 DEFINITIONS

Effective Date: 11/22/2019

See the **ADS Glossary** for all ADS terms and definitions.

**anti-ram**
Description of a barrier meeting the specification for anti-ram, SD-STD-02.01; sufficient, at the maximum threat, to arrest a 15,000 lb. (6810 kg) gross-weight vehicle traveling at a maximum of 50 mph (80 km) perpendicular to the barrier. (**Chapter 562**)

**armored vehicle**
A conveyance modified by armor systems, which are designed to defeat multiple impacts of ballistic rounds. Specific types of opaque and transparent armor are applied to the vehicle without noticeably changing its outward appearance. (**Chapter 562**)

**authorized classified conversations**
The levels of classified discussion permitted by standard on a secure voice installation in CAA facilities. (**Chapter 562**)

**ballistic resistance or ballistic-resistant (BR)**
Products and designs certified by DS/PSP/PSD under the provisions of SD-STD-01.01 (see **12 FAH-5 H-011**, subparagraph (4)) to withstand a minimum of 7.62/5.56 mm rifle rounds fired from approximately 20 feet (6 m) without penetration or spalling. (**Chapter 562**)

**Classified National Security Information (Classified Information)**
Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked (confidential, secret, or top secret) to indicate its classified status when in documentary form. It is also referred to as classified information.

**a.** Confidential: Information, of which the unauthorized disclosure could reasonably be expected to cause damage to the national security that the original classification authority is able to identify or describe.

**b.** Secret: Information, of which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

**c.** Top Secret: Information, of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. (**Chapters 545**, **552**, **562**, **566**, **567**)

**compound access control (CAC)**
System of gates, barriers, and guard booths used to pre-screen personnel and vehicles entering a secure perimeter. (**Chapter 562**)

**controlled access area (CAA)**
A specifically designated area within a building where classified information may be handled, stored, discussed, or processed. There are two types of CAAs: core areas and restricted areas. (**Chapter 562**)

**emergency exit**
A secure door designated for emergency egress during a fire or other life threatening evacuation. (**Chapter 562**)

**forced entry (FE)**
All references to forced entry (FE) in this chapter refer to the criteria set forth in SD-STD-01.01, Revision G (Amended), Certification Standard - Forced Entry and Ballistic Resistance of Structural Systems. See **12 FAH-5 H-031**, subparagraph (4). (**Chapter 562**)

**hardline**
Term referring to a system of barriers surrounding a protected area which affords degrees of forced entry, ballistic resistant, or blast protection, or combinations of these three. A hardline may include walls, floors, ceilings, roofs, windows, doors, or non-

window openings, all of which must provide the level of protection specified for that hardline. (**Chapter 562**)

**interior hardline**
Hardline separating the public access area from general work areas. The interior hardline typically includes the public access control (PAC) area (see **12 FAH-5 H-452.1**).

Overseas Security Policy Board (OSPB) was created by Presidential Decision Directive/NSC-29, which transferred the functions of the Overseas Security Policy Group (OSPG) to the OSPB and designated the Director of the Diplomatic Security Service to chair the OSPB. The OSPB charter, which superseded the OSPG charter (signed April 15, 1986), was approved by its membership on July 19, 1995. (**Chapter 562**)

**public access control (PAC)**
An area provided for the screening of visitors and employees before admittance into areas behind the hardline (see **12 FAH-5 H-452.1**). (**Chapter 562**)

**restricted areas**
Areas of the building in which classified information may be handled and stored. Classified discussions and processing are permitted but may be limited to designated areas, depending on the technical security threat. (**Chapter 562**)

**safe area**
A designated area within a building that serves as an emergency sanctuary and provides at least 15-minute forced-entry and ballistic-resistant (FE/BR) protection, emergency power, ventilation, communications, and emergency egress. (**Chapter 562**)

**safe haven**
A designated area within a building that serves as an emergency sanctuary and provides at least 60-minute forced-entry and ballistic-resistant (FE/BR) protection, emergency power, ventilation, communications, and emergency egress. (**Chapter 562**)

**security container**
A container (safe) that houses a built-in, three position, dial-type combination lock and is approved by the General Services Administration (GSA) for storage of classified information. (**Chapter 562**)

**sensitive but unclassified information (SBU)**
SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information, (TL;DS-61;10-01-199), 12 FAM 541 Scope, (TL;DS-46;05-26-1995).

SBU information includes, but is not limited to:

- Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and

- Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. (**Chapter 545** and **562**)

**surge capacity**
Space required to manage a sudden, unexpected increase in personnel that would otherwise severely challenge or exceed the current capacity of the existing office space. (**Chapter 562**)

**swing space**
Temporary office or special space used while renovations or capital improvements are underway or when new space is being acquired. (**Chapter 562**)

562_112219