Functional Series 500 – Management Services
ADS 562 – Physical Security Programs (Overseas)

Table of Contents

ADS 562 - Physical Security Programs (Overseas)

562.1 OVERVIEW

This chapter identifies the overseas physical security policy for the protection of USAID employees, facilities, and national security and sensitive information.

562.2 PRIMARY RESPONSIBILITIES

a. The Office of Security (SEC) has primary responsibility for interpreting, supplementing, and developing physical security policy and for oversight of USAID office physical security enhancements.

b. Bureaus and Missions are responsible for notifying SEC when any action is contemplated that will affect USAID use of office space.

c. USAID Senior Managers (Assistant Administrators, Mission Directors, USAID Representatives, Independent Activity Directors, and Office Directors) are responsible for ensuring that all employees and contractors coming under their authority are aware of and follow the USAID security policies and procedures contained in this ADS Chapter.

d. Unit Security Officers (USOs) are responsible for coordinating security activities within their respective USAID Mission or USAID/W Bureau. **(See ADS 561.3.3c)**

e. All USAID employees and contractors are responsible for complying with USAID security policies and procedures as reflected in this ADS Chapter.

f. The Executive Secretariat is responsible for notifying SEC/PSP (Physical Security Programs Division) in advance of any overseas travel by the A/AID or DA/AID. **(See 562.3.9)**

562.3 POLICY AND PROCEDURES

562.3.1 Office Building Security

SEC must be notified of any potential action that may affect the use of office space, such as

- USAID openings, closings, or relocations;
- Staff increases or decreases; or
- Other activities necessitating changes in the physical security provisions for office space.

USAID Bureaus, Offices, 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/PSP. This requirement is in addition to the Bureau for Management, Office of Administrative Services, Overseas Management Support Division (M/AS/OMS) approval required by 6 FAM 732. **(See Mandatory References, 12 FAM 300 and 6 FAM 732)**

Prior to lease approval by M/AS/OMS, SEC must ensure that a site survey is performed to determine whether the facility can be brought up to the minimum security standards described in 12 FAH 5 and 6.

SEC designs and installs physical security systems in consultation with the USAID Director's or Representative's staff, the Regional Security Officer (RSO), and other appropriate offices in Washington.

562.3.2 Physical Security Standards

All physical security standards must be met in new office buildings (NOBs), newly acquired buildings (NABs), and other functional space whether acquired by purchase, long-term lease, or short-term lease, unless otherwise specified in the Department of State (DOS) standards of 12 FAH 5 and 6. This policy applies to stand-alone facilities, commercial office space, and embassy/consulate buildings and annexes. USAID Missions must not occupy new facilities until written approval is granted by SEC.

The standards in 12 FAH-5 and 12 FAH-6 are modified for USAID as follows:

- 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 grills, 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 a commercial office building. The percentage refers to the square-footage of the space occupied in the building and to the ratio of USAID staff in the building.

- USAID safe areas and safehavens must accommodate a minimum of 50 percent of the USAID staff and be designed for a minimum of 10 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 (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, and metal and package screening devices.

562.3.3 Exception Requests

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

Missions initiating an exception request must cable the request to SEC/PSP for clearance and ultimate delivery to the State Department's Diplomatic Security Division for final approval. Exception requests must include the following:

a. Identification of the specific standard(s) to be waived;

b. Justification for the exception;

c. Statement of Agency operational requirements;

d. Permits;

e. Site plan, maps, and photographs;

f. Floor plan;

g. Description of the building;

h. Description of existing security measures; and

i. Chief of Mission (COM) and RSO comments and recommendations.

SEC must evaluate the package for completeness and technical viability. The SEC evaluation will be forwarded to M/AS/OMS and the applicable Bureau for comments. It will then be sent to the Administrator for approval/disapproval before being forwarded to Diplomatic Security for a final decision.

562.3.4 USAID Internal Security Procedures

USAID Mission Directors must have written security procedural guides and use them to ensure that their physical security systems and other security measures are effectively employed. The guides must outline routine and emergency security actions and assign specific security responsibilities to individual employees. The development of the procedural guide must be coordinated with the RSO. The Overseas Security Procedures Guide is provided as a sample guide. **(See Additional Help, Overseas Security Procedures Guide)**

USAID Mission Directors and Representatives are required to hold, at a minimum, semiannual security drills to practice emergency procedures in the event of a fire, bomb threat, or civil disturbance.

562.3.5 Overseas Security Budget and Funding

Overseas security budget and funding must be handled in accordance with the policies and procedures outlined in this chapter.

USAID Bureaus, Offices, and Missions must provide their annual security program requirements to SEC via cable using the USAID R4 process.

SEC consolidates approved, USAID worldwide security requirements into the USAID R4 process as part of the SEC annual budget request. Based on the budget allowances received by SEC, SEC administers and provides requisite funding and security equipment to secure newly acquired buildings, new office buildings, and additional office space that have been approved for lease or purchase by M/AS/OMS, the respective geographic Bureau, and SEC.

USAID 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/AS/OMS, the respective geographic Bureau, and SEC.

Missions are responsible for funding all unprogrammed residential security costs that may evolve from increased personnel staffing.

562.3.6 Overseas Residential Security and Local Guard Programs

The Department of State administers the Overseas Residential Security and Local Guard Programs through the RSO at post. Refer to 2 FAH-6, which is maintained by the RSO. USAID participation in these programs is in accordance with the policies and procedures contained in this chapter.

Prior to leasing or purchasing a residence, the USAID Executive Officer (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.

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

All requests for 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

Department of State funding for the residential security program applies only to U.S. direct-hire 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.

USAID 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 program funds accordingly.

562.3.8 Security Equipment Accountability, Control, and Maintenance

Record Keeping: All physical security equipment must be recorded in the USAID property books and controlled in accordance with the provisions of 6 FAM 220 and ADS 534, Personal Property Management Overseas. **(See Mandatory References, 6 FAM 220 and ADS 534)**

Accountability: Missions are accountable for all SEC-funded security equipment. This equipment is considered Nonexpendable Property (NXP), with the exception of certain low-dollar-value, nonserialized items such as mechanical locks. All NXP security equipment must be entered into the USAID property account regardless of the funding source or whether used by direct-hire employees or contractors. In case of a staff reduction or USAID closure, SEC must provide disposition instructions. Copies of property survey reports for lost and stolen security equipment must be provided to SEC.

Maintenance: Missions must maintain all physical security equipment provided by SEC. The Unit Security Officer (USO) must ensure that preventive maintenance is applied to all systems.

The RSO must be notified by the USOs when maintenance needs are beyond the capabilities of the USAID staff. Arrangements will be made to obtain the assistance of a Security Engineering Maintenance Program (SEMP) team. In the event that the RSO cannot provide assistance within a reasonable period of time, the USO may contact SEC for assistance.

562.3.9 Security of Administrator During Travel

The Office of Security, Physical Security Programs Division (SEC/PSP) must 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. The security of these officials must be accomplished in accordance with the policies and procedures outlined in this chapter.

The Executive Secretariat must notify SEC by memorandum in advance of the proposed travel. This memorandum must list the senior participants, proposed itinerary, and trip objectives.

SEC provides recommendations about security requirements and coordinates with appropriate entities for the provision of protective escorts, security guidance and enhancements, and individual briefings.

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

562.3.10 Locks, Keys, and Combination Controls

Locks, keys, and combination controls within USAID must be handled in conformance with the policies and procedures outlined in this chapter and 12 FAM. RSO approval is required prior to the installation, modification, or removal of any security locking devices used for the protection of National Security Information and all entrance and exit doors in any USAID facility. (For Missions that are authorized storage of classified materials, refer to 12 FAM 446, Building Security - Lock and Leave (L&L) Policy.) **(See Mandatory Reference, 12 FAM 446)**

a. Keys: Principal and alternate Key Custodians must be appointed for each USAID office.

The Key Custodian must conduct a quarterly key inventory. The inventory results must be available for SEC inspection.

Accountable keys must be marked "US Govt - Do Not Dupl". Cutting codes or other markings that could aid a locksmith in duplicating keys must be stored in a security container for reference.

b. Combinations: The combinations on all security equipment must be changed under the same criteria as that used for combinations on security containers as stipulated in 12 FAM 532, Locks. The Unit Security Officer must maintain a central record of all combinations within the USAID mission and must ensure that the RSO is provided a copy of the up-to-date central record. **(See Mandatory Reference, 12 FAM 532)**

562.3.11 Terrorist and Criminal Incident Reporting

All terrorist and criminal incidents affecting USAID employees, contractors, and their dependents (overseas) must be reported by the mission to SEC after appropriate local notification of the RSO. The USAID/W Duty Officer must always be notified.

When a serious incident occurs, missions must immediately telephone the USAID/W Duty Officer. The USAID/W Duty Officer in turn notifies the SEC Duty Officer. A follow-up telegram must be forwarded to SEC within one workday after the incident. Requirements for handling classified information must be followed at all times.

At overseas Missions, reports by telephone, telegram, and memorandum must include the following:

- A summary of the incident;
- Date and local time 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; and
- Response of host government forces.

562.4 MANDATORY REFERENCES

562.4.1 External Mandatory References

a. **6 FAM 220, Personal Property Management**

b. **6 FAM 732, Leasing Policy**

c. **12 FAM 300, Physical Security Programs**

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

e. **12 FAM 532, Locks**

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

g. 12 FAH-6, Department of State, OSPB Security Standards and Policy Handbook

562.4.2 Internal Mandatory References

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

b. **ADS 561, Security Responsibilities**

562.5 ADDITIONAL HELP

Overseas Security Procedures Guide

562.6 DEFINITIONS

The terms and definitions listed below have been included into the ADS Glossary. See the ADS Glossary for all ADS terms and definitions. (See ADS Glossary)

access
The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access by being in a place where national security information is kept, processed, handled, or discussed, if the security control measures that are in force do not prevent that person from gaining knowledge of such information. (Chapters 562, 566, 567, 568)

ballistic resistance
The capacity of security barriers to defeat a variety of handgun, shotgun and rifle rounds. (Chapters 562, 563)

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

forced entry resistance
The capacity of security barriers to resist mob attack as outlined in Department of State Certification Standard SD-STD-01.01, Forced Entry and Ballistic Resistance of Structural Systems. (Chapter 562)

***Sensitive But Unclassified information (SBU)**
A category of unclassified official information and material that is not national security information, and therefore is not classifiable, but nevertheless requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of the Agency to accomplish its mission, proprietary data, records requiring protection under the Privacy Act, and data not releasable under Sections 552 and 552a of Title 5 of the Freedom of Information Act.

SBU information includes, but is not limited to, information received through privileged sources and certain personnel, medical, personnel, commercial, and financial records, 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 individual privacy, Federal programs, or foreign relations. (source: 12 FAM 540)

Examples of SBU include travel of agency employees to or through a high or critical terrorist threat environment; investigatory records compiled by an agency conducting lawful national security intelligence investigation (source: FOIA); and candid assessments of situations in a host country which could cause embarrassment if made public. Material of this type, which requires protection and limited dissemination, shall

be designated by any official having signing authority for the material. (Chapters 545, 552, 562, 566, 567)

562_042502_w091003