ADS Chapter 562

Physical Security Programs (Overseas)

Revision Date: 08/09/2006
Responsible Office: SEC/OD
File Name: 562_080906_cd45

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

***This chapter has been substantively revised in its entirety.**

Table of Contents

ADS 562 - Physical Security Programs (Overseas)

562.1 OVERVIEW

Effective Date: 7/1/2006

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: 7/1/2006

a. The **Office of the Administrator (A/AID) staff** is responsible for notifying the Office of Security, Division of Physical Security Programs (SEC/PSP) 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 security policy directives and required procedures, and for oversight of physical and technical security enhancements for USAID offices.

c. **Bureaus/Offices 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. **Unit Security Officers (USOs)** are responsible for coordinating and monitoring security activities within their respective USAID Mission or USAID/W Bureau/Office. (see **ADS 561.3.3c**)

f. **All 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, Overseas Management Staff (M/OMS)** is responsible for approving the lease or purchase of USAID overseas office space.

562.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 7/1/2006

562.3.1 Overseas Office Building Security

Effective Date: 7/1/2006

a. Bureaus/Offices and Missions must notify the Office of Security (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**.**

Bureaus/Offices 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 USAID Mission outside a controlled access area. Missions initiating a proposal to receive, store, process, or discuss classified national security information must cable the request to SEC/PSP 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 or SEC must conduct a site survey. Both SEC and DS must approve this survey prior to implementation of any system.

c. **Leases:** 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, Overseas Management Staff (M/OMS) approval required by **15 FAM 312**. Prior to lease approval by M/OMS, SEC must ensure that a security assessment is performed to determine whether the facility can be brought up to the minimum security standards described in **12 FAH-5 and -6**.

d. **Physical security systems:** SEC designs and installs physical security systems in consultation with USAID Directors or Representatives, the Regional Security Officer (RSO), and other appropriate offices in USAID/Washington.

562.3.2 Physical Security Standards

Effective Date: 7/1/2006

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 security standards contained in this ADS chapter and Department of State (DOS) standards 12 FAH-5 and -6, unless otherwise specified therein. This policy applies to stand-alone facilities, commercial office space, embassy/consulate buildings, and annexes. USAID Missions must not occupy new facilities until SEC grants them written approval.

b. SEC has modified the standards in 12 FAH-5 and 12 FAH-6 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 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 Nationals (FSN) employees, exceed 50 percent of the total building staff population.
- 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 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: 7/1/2006

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. Bureaus/Offices 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.

c. 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 initiating an exception request must cable the request to SEC/PSP for clearance and ultimate delivery to the State Department's Bureau of Diplomatic Security 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; (Building Plans)

(g) Description of the building;

(h) Description of existing security measures; and

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

d. SEC must evaluate the package for completeness and technical viability. Next, SEC must forward the evaluation to M/OMS and the applicable Bureau/Office for comments. SEC must then send the request to the Administrator for approval/disapproval before it is sent to DS for a final decision.

562.3.4 USAID Internal Security Procedures

Effective Date: 7/1/2006

a. 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, assign specific security responsibilities to individual employees, and complement the Embassy's Emergency Action Plan (EAP). Mission Directors must coordinate the development of the procedural guide with the RSO. See **Overseas Security Procedures Guide** for a sample guide.

b. USAID Mission Directors and Representatives must hold, at a minimum, semi-annual 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

Effective Date: 7/1/2006

Overseas security budget and funding must be handled in accordance with these policy directives and required procedures:

- USAID Bureaus/Offices and Missions must provide their annual security program requirements, including physical security and security communication equipment, armored vehicles, and investigation requirements, to SEC via cable using the USAID Annual Report process. See **ADS 202.3.7.4** and each year's Annual Report Guidance.

- SEC consolidates approved, USAID worldwide security requirements into the USAID Annual Report process as part of the SEC annual budget request. Based on SEC's budget allowances, 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/OMS, the respective geographic Bureau/Office, 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/Office, 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

Effective Date: 7/1/2006

The Department of State administers the Overseas Residential Security and Local Guard Programs through the Regional Security Officer (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 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 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, USAID 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 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

Effective Date: 7/1/2006

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. 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 arrange funds accordingly.

562.3.8 Security Equipment Accountability, Control, and Maintenance

Effective Date: 7/1/2006

a. **Record Keeping:** Missions must record all physical security equipment in the USAID property books and control equipment, 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 Nonexpendable 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, 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:

- Missions must budget for the maintenance of all physical security equipment provided by SEC.

- The Unit Security Officer (USO) must ensure that all systems receive preventive maintenance.

- The USO must notify the RSO and SEC/PSP when maintenance needs are beyond the capabilities of the USAID staff.

- In response to Mission requests, the RSO will obtain the assistance of a Security Engineering Officer.

- 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 Locks, Keys, and Combination Controls
Effective Date: 7/1/2006

a. Locks, keys, and combination controls within USAID: These must conform with the following policy directives and required procedures and 12 FAH-5 G.45.2:

(1) RSO approval is required prior to the installation, modification, or removal of any security locking devices used for the protection of classified national security information, and all entrance and exit doors in any USAID facility.

(2) For Missions that are authorized for storage of classified materials, refer to **12 FAM 446, Building Security - Lock and Leave (L&L) Policy**.

b. **Keys:** Mission Directors must appoint principal and alternate Key Custodians for each USAID office.

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

(2) 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.

c. **Combinations:** The combinations on all security equipment must be changed under the same criteria 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 has a copy of the up-to-date central record.

562.3.10 Security of the Administrator during Travel

Effective Date: 7/1/2006

a. The Office of Security, Physical Security Programs Division (SEC/PSP) 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. The Office of the Administrator (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 (i.e., Mission Executive Officers and RSOs) to supply protective escorts, security guidance and enhancements, 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: 7/1/2006

a. The Mission must report to SEC all terrorist and criminal incidents affecting USAID employees, contractors, and their dependents (overseas) after notifying the appropriate local RSO. The Mission must also notify the State Operations Center.

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**)

A serious incident may include, but is not limited to, those which affect the operational status of the 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 memorandum 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.

562.4 MANDATORY REFERENCES

Effective Date: 7/1/2006

562.4.1 External Mandatory References

Effective Date: 7/1/2006

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

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

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. 14 FAM 410, Personal Property Management for Posts Abroad

g. 15 FAM 312, Leasing Policy

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

562.4.2 Internal Mandatory References

Effective Date: 9/28/2005

a. ADS 202, Achieving (section 3.7.4)

b. ADS 534, Personal Property Management Overseas

c. ADS 561, Security Responsibilities

d. ADS 568, National Security Information and Counterintelligence Security Program

e. Annual Report Guidance, FY 2006

562.5 ADDITIONAL HELP

Effective Date: 9/28/2005

a. Overseas Security Procedures Guide (Reserved)

562.6 DEFINITIONS

Effective Date: 9/28/2005

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)

Classified National Security Information (Classified Information)
Information that has been determined pursuant to EO 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, the unauthorized disclosure of which reasonably could 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)

controlled access area
Specifically designated area within a building where classified information may be handled, stored, discussed, or processed. There are two types of controlled access areas: core and restricted. Those areas of a building requiring the highest levels of protection where intelligence, cryptographic, security and other particularly sensitive or compartmentalized information may be handled, stored, discussed, or processed. 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)

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)

hardline
Term referring to an overseas system of barriers surrounding a protected area which may afford degrees of forced entry, ballistic resistance or blast protection. A hardline may include walls, floors, ceilings, roofs, windows, doors, or non-window openings, all which must provide the level of protection specified for the threat category and facility designation. (Chapter 562)

safehaven
A designated area within a building that serves as an emergency sanctuary and provides at least 60-minute force-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 fourth 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, 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_080906_w081506_cd45