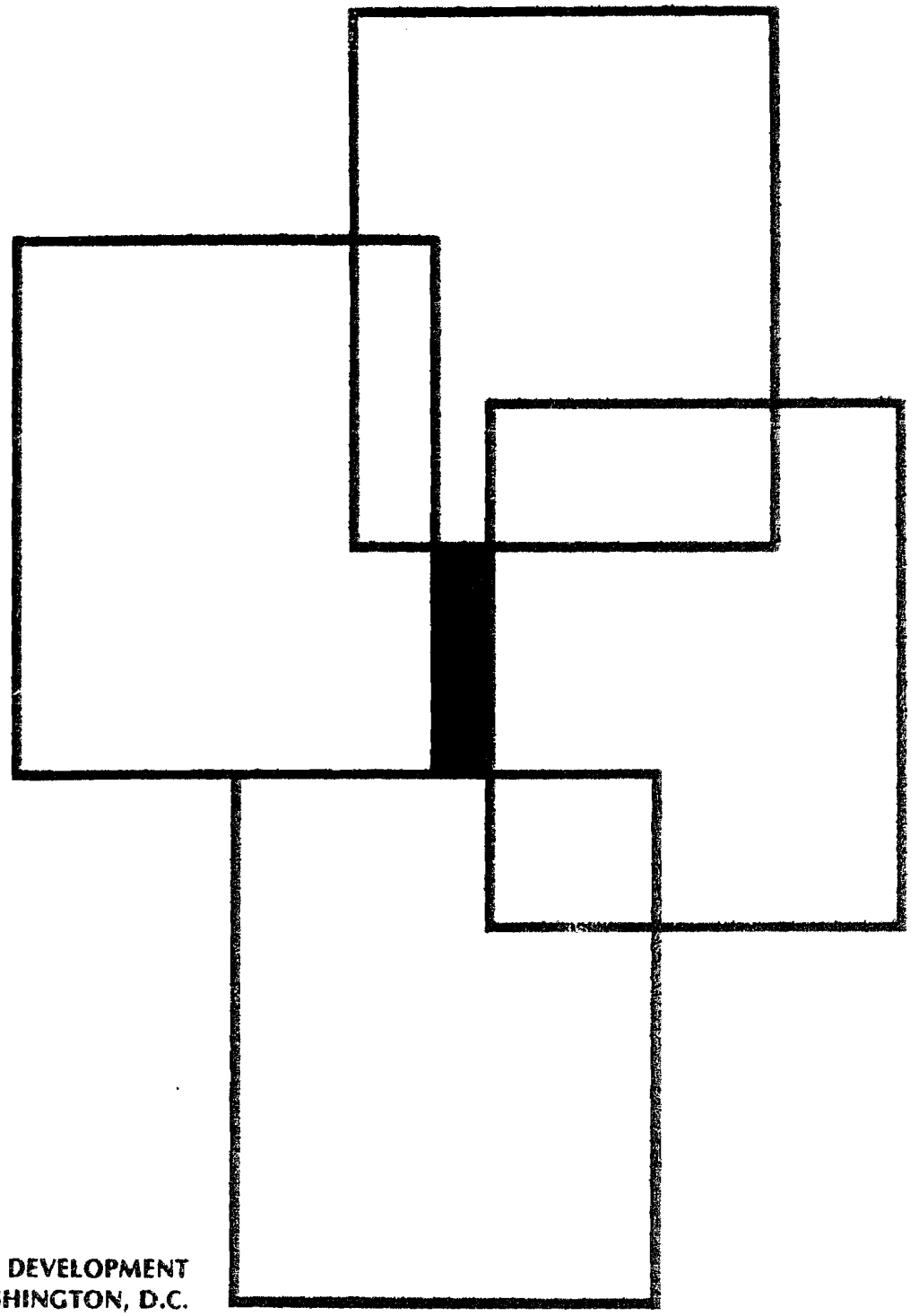
Security



AGENCY for INTERNATIONAL DEVELOPMENT
WASHINGTON, D.C.

AGENCY FOR INTERNATIONAL DEVELOPMENT

HANDBOOK TRANSMITTAL MEMORANDUM	DATE July 3, 1989	TRANS. MEMO NO. 6:26

MATERIAL TRANSMITTED:

Handbook 6 - Security

Handbook 6 has been reissued in its entirety.

SUPERSEDES:

Handbook 6 in its entirety (TMs 6:1, 6:2, 6:8, 6:14, 6:15, 6:16, 6:20, 6:21, 6:24, 6:25).

FILING INSTRUCTIONS:

1. Remove superseded material as indicated under SUPERSEDES.
2. File the attached in their appropriate places.
3. Initial the Transmittal Memorandum Checksheet (in the back of the Handbook binder) beside TM 6:26.

* * * * * * *

KEEP THIS TRANSMITTAL MEMORANDUM, which has an up-to-date Checklist for this Handbook on the back. File this TM 6:26 in the front of the handbook binder; discard TM sheet 6:25.

* * * * * * *

Address questions about this Handbook to IG/SEC.

For additional copies of this Transmittal contact M/SER/IRM/PE.

CHECKLIST FOR HANDBOOK 6
SECURITY

AUTHOR OFFICE: IG/SEC

DATE	MATERIAL TRANSMITTED	TM NO.
6-28-89	Complete Handbook	6:26

HANDBOOK 6

SECURITY

TAB I PERSONNEL SECURITY CLEARANCE PROGRAM

Chapter 1 - Security Clearances for Agency Employees

Chapter 2 - Security Clearances for Contractors and Contract Personnel

TAB II INFORMATION SECURITY PROGRAM

Chapter 3 - Information Security Program

Chapter 4 - (Reserved)

TAB III AID WASHINGTON SECURITY PROGRAM

Chapter 5 - AID Washington Security Program

Chapter 6 - (Reserved)

TAB IV OVERSEAS SECURITY PROGRAM

Chapter 7 - Security Responsibilities Overseas

Chapter 8 - USAID Office Building Physical Security

Chapter 9 - Security Procedures

Chapter 10 - Operations Security

Chapter 11 - Security Communications

Chapter 12 - Armored Vehicles

Chapter 13 - Residential Security

Chapter 14 - Local Guards

Chapter 15 - Construction and Transit Security (Reserved)

Chapter 16 - (Reserved)

TAB V SECURITY AWARENESS AND TRAINING PROGRAM

Chapter 17 - Counterintelligence Awareness

Chapter 18 - Security Awareness and Education

Chapter 19 - Security Procedures Training

Chapter 20 - (Reserved)

Chapter 21 - (Reserved)

TAB VI INSPECTIONS AND REPORTING PROGRAM

Chapter 22 - USAID Security Inspections

Chapter 23 - USAID Incident Reports

HANDBOOK 6

TABLE OF CONTENTS

TAB I - PERSONNEL SECURITY CLEARANCE PROGRAM

Chapter 1 - Security Clearances for AID Employees

1A - Authorities..... 1-1
1B - Purpose..... 1-2
1C - Definitions..... 1-2
1D - Scope..... 1-7
1E - Policies..... 1-7
1F - Personnel Security Program Standards..... 1-9
1G - Personnel Security Procedures and Responsibilities..... 1-11
1H - Exceptions..... 1-14
1I - Participating Agency Service Agreements (PASA)/ Resources Support Services Agreements (RSSA) Employees..... 1-17
1J - Waivers of Pre-Appointment Investigations..... 1-19
1K - Rejection of Applicants for Sensitive Positions on Security Grounds..... 1-20
1L - Rejection of Applicants for Sensitive Positions on Suitability Grounds..... 1-20
1M - Denial, Suspension and Termination of Security Clearances..... 1-21
1N - Administrative Withdrawal of Security Clearance..... 1-21
1O - Restricting Access to Classified Material..... 1-21

Chapter 2 - Security Clearances for Contractor and Contract Personnel

2A - Authorities..... 2-1
2B - Purpose..... 2-1
2C - Background..... 2-2
2D - Definitions..... 2-2
2E - Scope..... 2-4
2F - Policies..... 2-4
2G - Security Clearance Forms..... 2-6
2H - Clearance Procedures and Responsibilities..... 2-7
2I - Revalidation or Extension of Clearances..... 2-10
2J - Reinvestigations for Changes in Position Sensitivity..... 2-10

Page

2K - Adverse Action Procedures..... 2-11
2L - Security Briefing and Termination Statements.... 2-11
2M - Exceptions..... 2-12

TAB 2 - INFORMATION SECURITY PROGRAM

Chapter 3 - Information Security Program

3A - Authorities..... 3-1
3B - Purpose..... 3-1
3C - Policy..... 3-1
3D - Responsibilities..... 3-2

Attachment 3A - AID Original Secret Classification Authorities
Attachment 3B - AID Original Confidential Classification Authorities
Attachment 3C - AID Declassification Authorities

Chapter 4 - Reserved

TAB 3 - AID WASHINGTON SECURITY PROGRAM

Chapter 5 - AID Washington Security Program

5A - Authorities..... 5-1
5B - Purpose..... 5-1
5C - Scope..... 5-1
5D - Responsibilities..... 5-1
5E - Policy..... 5-1
5F - Building Security..... 5-2
5G - Identification Cards..... 5-3
5H - AID/W Locks/Combinations..... 5-5
5I - AID/W Emergency Situations..... 5-5

Chapter 6 - Reserved

TAB IV - OVERSEAS SECURITY PROGRAM

Chapter 7 - Security Responsibilities and Relationship at Overseas Posts

7A - Authorities..... 7-1

Page

7B - Purpose..... 7-1
7C - Responsibilities..... 7-1
7D - AID - State Overseas Security Agreement..... 7-2

Attachment 7A - The Agency for International Development/Department of State Overseas Security Agreement

Chapter 8 - USAID Office Building Physical Security

8A - Authorities..... 8-1
8B - Purpose..... 8-1
8C - Definitions..... 8-1
8D - Policy..... 8-1
8E - Objective..... 8-2
8F - Physical Security Systems..... 8-2
8G - Accountability, Repair, Maintenance and Replacement..... 8-3
8H - Waivers..... 8-4

Chapter 9 - Security Procedures

9A - Authorities..... 9-1
9B - Purpose..... 9-1
9C - Definitions..... 9-1
9D - Policy..... 9-1
9E - Security Procedures..... 9-2

Attachment 9A - Security Controller Duties (Sample)

Chapter 10 - Operations Security

10A - Authority..... 10-1
10B - Purpose..... 10-1
10C - Objective..... 10-1
10D - Vulnerabilities..... 10-1
10E - OPSEC Measures..... 10-2
10F - Responsibilities..... 10-2

Chapter 11 - Security Communications

11A - Authorities..... 11-1
11B - Purpose..... 11-1
11C - Definitions..... 11-1
11D - Policy..... 11-2
11E - Responsibilities..... 11-5

Page

Chapter 12 - Armored Vehicles

12A - Purpose..... 12-1
12B - Definitions..... 12-1
12C - Objective..... 12-1
12D - Policy..... 12-2
12E - Maintenance and Funding..... 12-2
12F - Reassignment of Heavy Armored Vehicles..... 12-2
12G - Budgeting for LAVs..... 12-2

Chapter 13 - Overseas Residential Security

13A - Authorities..... 13-1
13B - Purpose..... 13-1
13C - Program Administration..... 13-1
13D - Department of State Policy..... 13-1
13E - AID Policy..... 13-2

Chapter 14 - Overseas Local Guard Program..... 14-1

14A - Authorities..... 14-1
14B - Purpose..... 14-1
14C - Program Administration..... 14-1
14D - Department of State Policy..... 14-1
14E - AID Policy..... 14-1

Chapter 15 - Construction and Transit Security (Reserved)

Chapter 16 - Reserved

TAB 5 - SECURITY AWARENESS AND TRAINING REQUIREMENTS

Chapter 17 - Counterintelligence Awareness

17A - Authorities..... 17-1
17B - Purpose..... 17-1
17C - Definitions..... 17-2
17D - Policy..... 17-3
17E - Responsibilities..... 17-3
17F - Guidance..... 17-5
17G - Reporting Requirements..... 17-5
17H - Compliance..... 17-6

Page

Chapter 18 - Security Awareness and Education

18A - Authorities..... 18-1
18B - Purpose..... 18-1
18C - Applicability..... 18-1
18D - Policy..... 18-1
18E - Responsibilities..... 18-2
18F - Department of State Sponsored Training..... 18-3
18G - AID Sponsored Training..... 18-4
18H - Training Records..... 18-5

Chapter 19 - Security Procedures Training

19A - Authorities..... 19-1
19B - Purpose..... 19-1
19C - Objective..... 19-1
19D - Applicability..... 19-1
19E - Security Personnel..... 19-1
19F - Responsibilities..... 19-1
19G - Policy..... 19-2
19H - Compliance..... 19-2

Chapter 20 - Reserved

Chapter 21 - Reserved

TAB 6 - INSPECTIONS AND REPORTING PROGRAM

Chapter 22 - USAID Security Inspections

22A - Authorities..... 22-1
22B - Purpose..... 22-1
22C - Applicability..... 22-1
22D - Scope..... 22-1
22E - Policy..... 22-1
22F - Reports of Inspection..... 22-2

Attachment 22A - Office of Security Inspection Report
Attachment 22B - Format for Initial USAID Response to Office of Security Inspection Report

Page

Chapter 23 - USAID Incident Reporting

23A - Purpose..... 23-1
23B - Applicability..... 23-1
23C - Serious Incident Reporting..... 23-1
23D - Other Incident Reporting..... 23-2
23E - Report Content..... 23-2
23F - Report Distribution..... 23-2

TAB I - PERSONNEL

SECURITY CLEARANCE PROGRAM

TAB 1

PERSONNEL SECURITY CLEARANCE PROGRAM

This part establishes the authorities, policies, procedures, and assigns responsibilities for the personnel security clearance program for all AID direct-hire, PASA/RSSA personnel, contractors and contractor employees. The goal of this program is to ensure that the employment, assignment to duties, or retention in employment of individuals is clearly consistent with the interests of the national security and AID goals and objectives.

TABLE OF CONTENTS

PERSONNEL SECURITY CLEARANCE PROGRAM

Chapter 1 - Security Clearances for AID Employees

Chapter 2 - Security Clearances for Contractors and Contractor Employees

CHAPTER 1

SECURITY CLEARANCES FOR AID EMPLOYEES

1A. Authorities

1. The Foreign Assistance and Related Agencies Appropriation Act, as enacted annually. The Act of August 26, 1950, 64 Stat. 476.

2. Executive Order 10450 of April 27, 1953, as amended by Executive Order 10491 of October 13, 1953, Executive Order 10531 of May 27, 1954, Executive Order 10548 of August 2, 1954, Executive Order 10550 of August 5, 1954, and Executive Order 11785 of June 4, 1974, as they relate to the AID personnel security program.

3. Executive Order 12356, "National Security Information," of April 6, 1982, as it relates to the classification and protection of national security information and material.

4. Title 18 of the United States Code, Section 793(f), as it relates to penalties for compromise of national security information and material.

5. Transmittal Memorandum No. 1 to OMB Circular No. A-71, and the Federal Personnel Manual, Chapter 732, as they relate to the establishment of a personnel security program for personnel associated with Federal information technology programs and systems.

6. Federal Personnel Manual, Chapter 736, as it relates (a) to personnel investigations for suitability and (b) to National Security Decision Directive 84 pertaining to polygraph examinations for unauthorized disclosures of national security information.

7. Federal Personnel Manual, Chapters 731 and 732, as they relate to the basic requirements for investigating and adjudicating suitability and security issues.

8. OMB Circular No. A-123, as it relates to the establishment of systems for controlling and documenting individual access to Government assets.

9. Director of Central Intelligence Directive No. 1/14 (DCID 1/14), as it relates to the requirements for access to sensitive compartmented information.

1B. Purpose

This chapter sets forth policy, fixes responsibilities, and prescribes procedures pertaining to the development, operation, and maintenance of a personnel security program for all AID direct-hire and PASA/RSSA personnel.

1C. Definitions

1. National Security

The term "national security" relates to the protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs, against or from espionage, sabotage, and subversion, and any and all other acts designed to weaken or destroy the United States.

2. Classified Information and Material

The term "classified information and material" relates to information and material that requires special protection against unauthorized and/or improper access, use, operation, manipulation, disclosure, alteration, or destruction, in the interest of national security.

3. Limited Official Use Information and Material

The term "limited official use information and material" relates to certain sensitive official information and material which is not national security information, but nevertheless warrants a degree of protection. Such information or material may include, among other things, information received through privileged sources and certain personnel, medical, investigative, commercial, and financial records.

4. Office of Security

The term "Office of Security" relates to a component of the AID Office of the Inspector General.

5. Automation Security Officer

The term "Automation Security Officer" relates to the person assigned security functions within AID's Office of Information Resources Management.

1C

6. Office of Personnel Management

The term "Office of Personnel Management" relates to a component of the AID Bureau for Personnel and Financial Management.

7. Information Technology

The term "information technology" relates to and includes all activities, information, and material formerly identified as automated data processing, ADP, automation, office information systems, word processing, computers, and telecommunications.

8. Access

The term "access" relates to the ability and opportunity to obtain knowledge of national security and/or limited official use information or to operate an information technology system.

9. Sensitive Position

The term "sensitive position" means any position in AID, the incumbent of which could bring about, because of the nature of the position, a materially adverse effect on national security and/or AID objectives and assets.

10. Special-Sensitive Position

The term "special-sensitive position" means any position in AID, the duties of which are determined to be at a level higher than "critical sensitive" because of the greater degree of damage that an individual by virtue of occupancy of the position could cause to the national security, or because the duties may entail access to sensitive compartmented information.

11. Critical-Sensitive Position

The term "critical-sensitive position" means any position in AID, the duties of which include, but are not limited to:

a. Access to national security information and material up to, and including, Top Secret;

b. Development or approval of war plans, plans or particulars of future or major or special operations of war, or critical and extremely important items of war;

c. Development or approval of plans, policies, or programs which affect the overall operations of a department or agency; i.e., policy-making or policy-determining positions;

d. Investigative functions, the issuance of personnel security clearances, or service on personnel security boards;

e. Fiduciary, public contact, or other functions demanding the highest degree of public trust;

f. Responsibility for planning, directing, coordinating, and implementing the AID information technology security program;

g. Responsibility for directing, planning and designing of information technology systems, including hardware and software, or

h. Access to an information technology system during its operation or maintenance in such a way as to afford the opportunity, and with a relatively high risk, for causing grave damage or realizing a significant personal gain.

12. Noncritical-Sensitive Position

The term "noncritical-sensitive position" means any other sensitive position in AID that does not fall within the definition of a critical-sensitive position. The duties of a noncritical-sensitive position include, but are not limited to:

a. Access to national security information and material up to, and including, Secret.

b. Participation in planning, directing, coordinating, and implementating information technology security programs, under the supervision and technical review authority of a critical-sensitive position.

c. Responsibility for directing, planning, designing, operating, or maintaining information technology systems, under the supervision and technical review authority of a critical-sensitive position.

d. Access to an information technology system during its operation or maintenance in such a way as to afford the opportunity, and with a relatively low risk, for causing significant damage or realizing significant personal gain, under the supervision and technical review authority of a critical-sensitive position to ensure the integrity of the information technology system.

1C

13. Nonsensitive Position

There are no "nonsensitive positions" within AID. The generic term "nonsensitive position" means any position that does not fall within the definition of a special-sensitive position, critical-sensitive position, or noncritical-sensitive position.

14. Security Clearance

The term "security clearance" relates to an administrative determination by an appropriate authority that the designated individual is eligible to have access to a specified level of national security information and material.

15. Need to Know

The term "need to know" relates to an administrative determination by the possessor of national security and/or limited official use information and material that a prospective recipient of that information and material has a requirement for access to, knowledge of, or possession of that information and material in order to perform tasks or services essential to the fulfillment of assigned duties.

16. Approval

The term "approval" relates to a favorable finding by IG/SEC, based on the results of an appropriate security investigation.

17. Security Investigation

The term "security investigation" relates to inquiries designed to develop information pertaining to an individual for use in determining whether or not the employment, assignment to duties, or continued employment of that individual is clearly consistent with the interests of national security and AID goals and objectives.

18. National Agency Check

A "national agency check (NAC)" consists of a security investigation that includes the following file searches for information relating to the suitability of an individual for employment, assignment to duties, or continued employment:

a. Federal Bureau of Investigation, United States Department of Justice, including name and fingerprint files.

b. United States Office of Personnel Management.

c. IG/SEC, Office of the Inspector General, AID

d. Office of Investigations, Office of the Inspector General, AID

e. Such other United States Government files and records as are appropriate on the basis of previous civilian or military employment with the United States Government.

19. National Agency Check and Inquiries

A "national agency check and inquiries (NACI)" consists of a security investigation that includes the file searches that make up the aforementioned NAC, plus written inquiries to previous employers, present employers, references, educational institutions, law enforcement agencies, and credit/marriage/divorce/birth/citizenship records on request, or to resolve issues.

20. Minimum Background Investigation (MBI)

A "minimum background investigation (MBI)" consists of the NACI described above, a mandatory credit search and field work for purposes of issue resolution.

21. Limited Background Investigation

A "limited background investigation (LBI)" consists of a subject interview, personal interviews with selected sources covering specific areas of the subject's background during the past 1-3 years, and written inquiries, record searches, and credit searches for a total of five years.

22. Background Investigation

A "background investigation (BI)" relates to a security investigation that includes the file searches and written inquiries that make up the aforementioned NACI, plus a subject interview, personal interviews with employers, references, associates, neighbors, and educational faculty members. The BI normally covers a subject's background during the past five years.

1C

23. Special Background Investigation

A "special background investigation (SBI)" consists of a subject interview, written inquiries, record searches, credit search, and personal interviews with selected sources covering specific areas of a subject's background during the past 15 years.

1D. Scope

The policies, responsibilities, procedures and requirements set forth in this chapter are applicable to all AID direct-hire personnel, including Presidential appointees requiring Senate confirmation, Executive appointees requiring White House approval, advisory committee members (even when serving without compensation), per diem employees, intermittent employees, temporary employees, and seasonal employees, whether or not they are United States citizens. This chapter is also applicable to employees serving under a Participating Agency Services Agreement (PASA) or Resources Support Services Agreement (RSSA). This chapter does not apply to personnel working in or on AID programs and activities under any of the various forms of service contracting agreements. Personnel security policies, responsibilities, procedures, and requirements for contractors and contractor employees are set forth in Chapter 2.

1E. Policies

1. Personnel Security Policy

It is AID policy that no individual is employed by AID unless that individual's employment is clearly consistent with the interests of national security and AID goals and objectives. This policy applies to all direct-hire United States citizens and individuals assigned under Participating Agency Services Agreements and Resources Support Services Agreements. Direct-hire non-United States citizens employed by AID overseas must meet the security clearance requirements established by the United States Department of State for the position the individual will encumber.

2. Special-Sensitive Position

It is AID policy that no individual is employed, assigned to duties, or retained as an employee in a special-sensitive position in AID unless that individual meets the security clearance requirements of a special background investigation (SBI) and has been issued the appropriate security clearance under Section 3(b) of Executive Order 10450 and DCID 1/14.

1E

3. Critical-Sensitive Position

It is AID policy that no individual is employed, assigned to duties, or retained as an employee in a critical-sensitive position in AID unless that individual meets the security clearance requirements of a background investigation (BI) and has been issued the appropriate security clearance under Section 3(b) of Executive Order 10450.

4. Noncritical-Sensitive Position

It is AID policy that no individual is employed, assigned to duties, or retained as an employee in a noncritical-sensitive position in AID unless that individual meets the security clearance requirements of a minimum background investigation (MBI) and has been issued the appropriate security clearance under Section 3(a) of Executive Order 10450.

5. Periodic Reinvestigation

It is AID policy that employees in special-sensitive, critical-sensitive, and noncritical-sensitive positions must be reinvestigated five years after placement and at least once each succeeding five years. This is accomplished through the conduct of inquiries designed to ensure that the employee meets the requirements with regard to character, reputation, fitness, loyalty, qualifications, and other pertinent factors.

6. Update Investigation

An "Update Investigation (UI)" consists of the same coverage as the previous investigation (MBI, LBI, BI and SBI) during the 13 to 60 month period since the previous investigation.

7. Special Investigation

A "Special Investigation (SI)" is conducted whenever derogatory information is received which bears directly upon the suitability or loyalty of an AID employee.

8. Issuance of Security Clearance Prior to Appointment/Reappointment

It is AID policy that no individual is employed or re-employed in a special-sensitive, critical-sensitive, or noncritical-sensitive position unless that individual's security clearance has been issued within the previous 90 days.

1F. Personnel Security Program Standards

1. Standards for Designation of Sensitive Positions

In rendering a determination as to whether a position is sensitive (special-sensitive, critical-sensitive, or noncritical-sensitive), the Administrator or his/her designee will utilize criteria issued by the United States Office of Personnel Management (OPM). The applicable Executive Orders and Federal Personnel Manual sections are cited under 1A; however, other factors than those specifically listed may enter into the determination on a position-by-position basis; i.e., factors considered are unique tasks and duties of the position in question, and the presence of other safeguards designed to reduce the risk that the incumbent could cause a materially adverse impact on national security or AID goals and objectives.

2. Standards for Security Determinations

The following factors shall be considered in rendering a determination as to whether employment with AID is clearly consistent with the interests of national security:

a. Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

b. Any deliberate misrepresentation, falsification, or omission of material facts.

c. Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

d. Any illness, including any mental condition, of a nature which in the opinion of competent medical authorities may cause a significant defect in the judgement or reliability of the individual, with due regard to the transient or continuing effect of the illness and the medical findings in such a case.

e. Any facts which furnish reason to believe that an individual may be subjected to coercion, influence, or pressure which may cause him/her to act contrary to the best interests of the national security or AID goals and objectives.

f. Lack of discretion with regard to information; such as, loose talking, carelessness in the custody of documents, or negligence in observing security regulations.

g. Commission of any act of sabotage, espionage, treason, sedition, or attempts thereat, or preparation thereof, or conspiring with, or aiding or abetting another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

h. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

i. Advocacy of the use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

j. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or subdivision thereof by unlawful means.

k. Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

l. Performing or attempting to perform his/her duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

m. Refusal by the individual, upon the grounds of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his/her alleged disloyalty or other misconduct.

3. Standards for Determining the Level of Security Investigations

Notwithstanding the provisions of paragraphs 1E and 1G of this chapter, the Administrator or his/her designee may require additional security investigations beyond those specifically required by this

1F3

chapter for the purpose of developing further information for determining whether an individual's employment by AID is clearly consistent with the interests of the national security and AID goals and objectives

4. Standards for Handling of Information from Security Investigations

Investigations conducted pursuant to this chapter are designed to develop personal information about an individual that is to be used solely for the purpose of determining whether the employment of that individual in AID is clearly consistent with the interests of the national security and AID goals and objectives. Unless classified, this personal information shall be protected as Limited Official Use data. Any other use of this personal information is strictly prohibited, except as specifically noted in 1F5.

5. Handling of Information Pertaining to Actual or Suspected Violations of Law

Notwithstanding the provisions of 1F4, whenever a security investigation develops information indicating an actual or suspected violation of law, that information shall be referred to the appropriate law enforcement authority.

1G. Personnel Security Procedures and Responsibilities

1. Designation of Sensitive Positions

The Administrator or his/her designee shall determine and designate each position as special-sensitive, critical-sensitive, or noncritical-sensitive. Periodically, but not less than once every five years, IG/SEC shall review each position in concert with the Office of Personnel Management and the Office of Information Resources Management, and shall recommend to the Administrator or his/her designee a sensitivity level for each position. The final determinations and designations rendered by Administrator or his/her designee shall be recorded by IG/SEC. The Office of Personnel Management shall maintain and distribute a listing of all position designations.

2. Requesting Security Clearances for Direct-Hire Citizens

All requests for security clearances for direct-hire United States citizens must be submitted to IG/SEC by the applicable personnel processing unit on a completed form AID 6-1, Request for Security Action accompanied by the following completed forms:

1G2

a. Form SF 86, Questionnaire for Sensitive Positions (original + one)

b. Form SF 87, Fingerprint Chart (two originals)

c. Form AID 6-85, Foreign Residence Data (original + one)

d. Form AID 610-14, Authority for Release of Information (original + one)

e. Form DS-1350, Certification of Birth Abroad of a Citizen of the United States of America (for applicant and/or spouse, when applicable) (original)

f. Form OF 174, Application for Employment as a Foreign Service National (only when the spouse of an applicant or the intended spouse of an employee is not a United States citizen) (original + one)

g. Form DSP-34, Supplement to Application for Federal Employment (when an employee marries a United States citizen) (original + one)

All forms submitted must be typed or printed with sufficient boldness and clarity to allow the successful scanning of the information by electronic media.

After reviewing the forms for completeness and clarity, IG/SEC shall conduct, or cause to be conducted, the required security investigation, except as specifically noted in paragraphs 1H1, 1H4, and 1H5. In the event the forms do not contain all of the required information or they are not legible, they will be returned to the requester for completion by the applicant. The security clearance for such individuals shall be issued by IG/SEC, as appropriate.

3. Requesting Security Clearances for Direct-Hire Non-U.S Citizens Overseas

Based on a security support agreement with the United States Department of State, the Department conducts security investigations of non-United States citizens employed with AID overseas, as provided in Chapter 7, ("Security Responsibilities and Relationships at Overseas Posts") and submits, as appropriate, a Certificate of Acceptability for Employment to the USAID. All requests for security clearances for individual direct-hire non-United States citizens must be submitted to the United States Department of State by the applicable personnel processing unit, as prescribed by the aforementioned security support agreement.

1G

4. Updating Security Clearances

a. Direct-Hire United States Citizens

IG/SEC has the responsibility to conduct security updating investigations on all U.S. direct-hire employees at least once every five years.

b. Direct-Hire Non-United States Citizens Overseas

The Regional Security Officer responsible for the issuance of Certificates of Acceptability for Employment for direct-hire non-United States citizens shall conduct periodic (not less than every five years) reinvestigations as prescribed by the aforementioned security support agreement.

5. Special Investigations

IG/SEC has the authority to conduct, as required, special investigations on employees on whom derogatory information is developed which bears directly upon the suitability or loyalty of the individual. The Director of Security or his/her designee shall determine if any special security investigative action is necessary to ensure that the individual's continued employment is consistent with the interests of the national security and AID goals and objectives. Whenever it is determined that further security investigation is warranted, IG/SEC shall conduct, or cause to be conducted, such security investigation as is appropriate to resolve the issue.

6. Revalidation of Security Clearance

a. Direct-Hire United States Citizens

All requests for revalidation of an individual direct-hire United States citizen's security clearance must be submitted to IG/SEC by the applicable personnel processing unit on a completed form AID 6-1, Request for Security Action. The Director of Security (AIG/SEC) or his/her designee shall determine if any further security investigative action is necessary to revalidate, or suspend, the individual's security clearance.

b. Direct-Hire Non-United States Citizens Overseas

All requests for revalidation of an individual direct-hire non-United States citizen's Certificate of Acceptability for Employment shall be submitted to the United States Department of State by the applicable personnel processing unit, as prescribed by the aforementioned security support agreement.

7. Requesting Security Clearances for Presidential Appointments Requiring Senate Confirmation

All requests for security clearances for individual Presidential appointees requiring confirmation by the United States Senate are initiated by the White House, and the required security investigations are conducted by the Federal Bureau of Investigation of the United States Department of Justice. The security clearance for such individuals shall be issued by IG/SEC based upon a review of a favorable background investigation.

8. Requesting Security Clearances for Executive Appointments Requiring White House Approval

All requests for security clearances for individual Executive appointees requiring White House approval are initiated by the Administrator or his/her designee, and the required security investigations are conducted, or caused to be conducted, by IG/SEC. Security clearances for such individuals shall be issued by IG/SEC based upon a review of favorable background investigations.

9. Requesting Security Clearances for Advisory Committee Members Serving without Compensation

All requests for security clearances for individual Advisory Committee Members serving without compensation are initiated by the applicable appointing authority or his/her designee, and the required security investigations are conducted, or caused to be conducted, by IG/SEC. Security clearances for such individuals shall be issued by IG/SEC, as appropriate.

1H. Exceptions

1. Interagency Transfer of Security Clearances and Investigative Information

IG/SEC may accept from another Federal agency the investigative findings and/or security clearances issued by that agency pertaining to

an AID employee or applicant, and may thereupon issue an appropriate AID security clearance without further investigation provided that:

a. the investigation was completed within the last 36 months and there has been no break in service in excess of 12 months;

b. the prior investigation meets the required scope and coverage standards and is compatible with the sensitivity of the position; and

c. the prior investigation discloses no unresolved information which reflects adversely on the applicant's suitability for employment, eligibility for a security clearance, or risk in terms of information technology systems.

2. Temporary Appointments of Nonprofessional Personnel

Civil Service Recruitment temporary appointments, not to exceed (NTE) 90 days, may be made in the complement of nonprofessional personnel established within the Office of Personnel Management prior to the submission of a request for security clearance and/or prior to the receipt of a security clearance. However, the request for security clearance must be submitted within three working days following the date of assignment to duties, and individuals so appointed shall not be granted access to classified and/or limited official use information and material, and/or to information technology systems.

3. Temporary Appointments of Resident Staff Overseas

Resident staff temporary appointments, not to exceed (NTE) 90 days, may be made at an AID Mission overseas prior to the receipt of a security clearance, provided that the appointee is a United States citizen, is the spouse of a full-time, direct-hire United States Government employee possessing a Top Secret security clearance to whom the appointee was married at the time of the employee's investigation, and that an official request for security clearance has been correctly completed and submitted to IG/SEC. The individual so appointed may be permitted access to classified information and material up to and including Secret, access to limited official use information and material, and access to the resources of an information technology system, as necessary in the performance of official duties. Such a temporary appointment may be extended for an additional 90 days by AID/Washington upon the written request of the USAID and with the written concurrence of IG/SEC.

1H

4. Conditional Appointments to Noncritical-Sensitive Positions

Conditional appointments, not to exceed (NTE) 90 days, may be made to noncritical-sensitive positions for individuals who have satisfactorily completed the National Agency Check (NAC) portion of the Minimum Background Investigation. The individual so appointed may be permitted access to classified information and material up to and including Secret, access to limited official use information and material, and access to the resources of an information technology system, as necessary in the performance of official duties. Such a conditional appointment may be extended for an additional 90 days by a Bureau Assistant Administrator or his/her deputy, or the head of a non-Bureau office or his/her deputy, upon the written request of the applicable supervising authority, and with the written concurrence of IG/SEC. Whenever such a conditional appointment is made, the appointee shall be notified of the conditions of his/her appointment by the Office of Personnel Management.

5. Conditional Appointments to Critical-Sensitive Positions

Conditional appointments, not to exceed (NTE) 90 days, may be made to critical-sensitive positions for individuals who have been the subject of a satisfactorily completed National Agency Check and Inquiries (NACI) portion of the background investigation. The individual so appointed may be permitted access to classified information and material up to and including Secret, access to limited official use information and material, and access to the resources of an information technology system, as necessary in the performance of official duties. Such a conditional appointment may be extended for an additional 90 days by a Bureau Assistant Administrator or his/her deputy, or the head of a non-Bureau office or his/her deputy, upon the written request of the applicable supervising authority, and with the written concurrence of IG/SEC. Whenever such a conditional appointment is made, the appointee shall be notified of the conditions of his/her appointment by the Office of Personnel Management.

6. Advisory Committee Members Serving without Compensation

IG/SEC may conduct, or cause to be conducted, security investigations as are clearly consistent with the interests of the national security and AID goals and objectives, in order to determine the suitability of Advisory Committee Members serving without compensation and requiring access to classified or limited official use information and material, and/or the resources of an information technology system.

1H

7. Consultants and Experts

Candidates who are appointed as consultants/experts in nonsensitive positions will be subject to a satisfactory completion of a post employment National Agency Check and Inquiries (NACI). No security clearance is required provided the candidate (1) has no access to classified or administratively controlled information; (2) performs services on a limited basis on AID premises (for administrative purposes, limited basis is arbitrarily defined as 15 days per calendar year); or (3) does not attend internal AID staff meetings. The AID 6-1 will clearly indicate the position is "nonsensitive."

II. Participating Agency Service Agreements (PASA)/Resources Support Services Agreements (RSSA) Employees

1. Security Clearance Requirements

AID security regulations apply to all personnel detailed or assigned to an AID program. No employee may be appointed or detailed to an AID - funded position until AID security requirements have been met. No payment will be made to an agency for services provided to AID unless the employee performing the service has been security approved in accordance with AID regulations. Responsibility for carrying out the security investigations rests with the participating agencies.

2. Security Clearance Procedures and Responsibilities

a. Overseas Assignments

(1) No security clearance is required for PASA/RSSA employees detailed to AID for 60 days or less in any 12 month period provided the PASA/RSSA (a) has no access to administratively controlled or classified information (i.e., generation, receipt, storage, or handling), (b) is not performing services on a regular basis on AID or Embassy premises, and (c) does not attend internal AID or Embassy staff meetings. The participating agency or AID Bureau has responsibility for notifying the PASA/RSSA's post of assignment that the employee does not possess a security clearance. The RSO and IG/SEC must be included as addressees in all such notification cables or correspondence.

(2) PASA/RSSA assignments of 60 days or less in any 12 month period require a NACI or background investigation when access to administratively controlled or classified material is required.

1I2a

(3) As a minimum, a NACI is required when the detail is between 60 and 129 days in any 12-month period.

(4) Employees providing services of 130 days or longer require a background investigation.

b. Services in the United States

(1) No security clearance is required for PASA/RASA personnel performing services outside of AID/W spaces, unless such persons will have access to administratively controlled or classified material. When access to administratively controlled or classified information is required, an appropriate NACI or background investigation must be conducted.

(2) No PASA/RSSA personnel may be assigned to work in any AID/W office unless that individual has had a NACI for a noncritical-sensitive position or a background investigation for a critical-sensitive position. All PASA/RSSA personnel working in AID spaces must have valid AID security clearances.

(3) Each AID/W Bureau or independent office using regularly assigned PASA or RSSA personnel in AID spaces will provide a list of such assignments to IG/SEC. The list will include the offices of assignment, names of employees, and be updated as changes occur.

3. Certification of PASA/RSSA Candidates

When a participating agency issues a security clearance on a PASA/RSSA candidate, that agency certifies clearance issuance on form AID 2-5, "Participating Agency Certification of Candidate's Qualifications." The form AID 2-5, accompanied by the candidate's current SF-86, "Questionnaire for Sensitive Positions," is forwarded to IG/SEC by the appropriate AID/W Bureau or independent office.

4. Clearance of Persons Acquired by Subcontract Under PASA/RSSA Agreements

To facilitate the clearance process, IG/SEC will conduct the investigations for security clearances of persons to be acquired by subcontract under PASA/RSSA agreements. Once identified, the participating agency will ensure that the candidate fills out the required security forms. Upon their completion, the candidate should make an appointment with IG/SEC to deliver the forms and be fingerprinted. If the forms are not complete, they will be returned to

1I4

the individual for modification. At the same time, the participating agency will execute form AID 2-5, "Participating Agency Certification of Candidate's Qualifications," and forward it to the appropriate AID Project Officer in the funding Bureau. The Project Officer must then execute an AID 6-10, "Request for Clearance," which must be countersigned by the Bureau's Executive Management Officer. The Project Officer must then submit both the AID 6-10 and the AID 2-5 to IG/SEC. Once the aforementioned forms are received from the Project Officer and candidate, IG/SEC will initiate the clearance process. When the clearance is granted, the PASA/RSSA employee will attend the AID security orientation session and subsequently be issued an ID card by IG/SEC.

5. Marriage of PASA Employees to Foreign Nationals

When a PASA employee marries a foreign national while serving abroad, the employee's security clearance must be revalidated. An appropriate investigation of the foreign spouse will be conducted by the Regional Security Officer on behalf of IG/SEC. The Director of the Mission to which the PASA employee is assigned is required to provide a written assessment of the marriage's impact on the national security. Upon completion of a favorable investigation, IG/SEC will revalidate the clearance.

6. Requests for Waivers of Pre-Appointment Investigations of PASA Employees

All requests for waivers to permit candidates to enter on duty on a PASA assignment pending completion of the appropriate investigation are initiated in the participating agency by the official authorized to sign Participating Agency Services Agreements, with sufficient information and justification to support a finding that the accelerated appointment is necessary in the national interest. The waiver request is submitted in accordance with the provisions of AID HB 12, to IG/SEC, which indicates in writing its comments for the AID Administrator's guidance. The waiver request, together with the Administrator's finding, is returned through the Office of Personnel Management to the participating agency and becomes a part of the employee's security file. When the appropriate investigation is satisfactorily completed, the participating agency so certifies to AID in accordance with 1I3.

1J. Waivers of Pre-Appointment Investigations

All requests for a waiver of required investigations for noncritical-sensitive and critical-sensitive positions shall be

1J

submitted to the Administrator by a Bureau Assistant Administrator or his/her deputy, or the head of a non-Bureau office or his/her deputy, with sufficient information and justification to support a finding that the accelerated appointment is necessary in the national interest. The waiver request is submitted through IG/SEC, which indicates in writing its comments for the Administrator's guidance. The waiver request, together with the Administrator's finding, becomes a part of the employee's security file.

1K. Rejection of Applicants for Sensitive Positions on Security Grounds

1. Appeal/Mitigation of Derogatory Information

A person being considered for a sensitive position is, whenever appropriate, given an opportunity to explain or refute derogatory personal information developed in an investigation before a decision is made on his/her security clearance. This practice prevents decision errors which might otherwise result from mistakes in identity or mitigating circumstances which are unknown to IG/SEC.

2. Consultation with Interested Bureaus and Offices

In the process of evaluating significant derogatory information which might lead to an adverse security finding, the Director of Security may consult with appropriate interested Offices and Bureaus before making a decision.

3. General Counsel Review

All adverse security decisions regarding applicants are reviewed by the Legal Counsel, Office of the Inspector General, to ensure against violation of their rights.

4. Notification of Rejection

Notification of nonselection is made to the applicant through the Office of Personnel Management.

1L. Rejection of Applicants for Sensitive Positions on Suitability Grounds

When significant adverse information is developed during a security investigation which has a bearing on an individual's suitability for employment, the Director of Security will make this information available to the Office of Personnel Management. Primary responsibility

1L

for a decision as to any adverse action rests with the Office of Personnel Management and will be made in accordance with the provisions of Handbook 25.

1M. Denial,Suspension and Termination of Security Clearances

PROCEDURES ASSOCIATED WITH THE ABOVE ACTIONS ARE BEING FORMALIZED. UPON COMPLETION, THEY WILL BE PROVIDED AS AN AMENDMENT TO THIS HANDBOOK.

1N. Administrative Withdrawal of Security Clearance

The security clearance of any person who is placed on LWOP for more than 60 days will be administratively withdrawn. In such instances, this action shall be without prejudice to the person's eligibility for a security clearance should the need again arise. Upon re-establishment of the need for access to classified information, a revalidation must be obtained from IG/SEC in accordance with the provisions of 1G6.

1O. Restricting Access to Classified Material

1. Access to classified material may be restricted on a temporary basis by IG/SEC where reasonable caution and prudence would indicate the need to take protective action. In all instances where IG/SEC places limitations on an employee's or PASA's access to classified material, the restrictions will remain in effect until relieved by IG/SEC. This decision may be influenced by a written justification from the USAID or AID/W Bureau/Office or a change in the conditions which prompted the restrictions. Examples of situations that may require protective action are:

a. Incumbents, including PASA's, of sensitive positions who marry non-U.S. citizens and are stationed in the country of the spouse's origin or former nationality;

b. Incumbents of sensitive positions whose spouses are employed by a foreign government or an instrumentality of a foreign government; and

c. Incumbents of sensitive positions who are naturalized citizens assigned to their country of origin.

CHAPTER 2

SECURITY CLEARANCES FOR CONTRACTOR AND CONTRACT PERSONNEL

2A. Authorities

1. The Foreign Assistance Act of 1961, Section 635(b), as amended, as it relates to contracts.

2. Executive Order 10865, as amended by Executive Order 10909, as it relates to the safeguarding of classified information within industry.

3. Transmittal Memorandum No. 1 to OMB Circular No. A-71, as it relates to the security of information technology systems operated on behalf of Federal agencies.

4. Department of Defense Regulation DOD 5220.22-R which sets policies, practices, and procedures for the Defense Industrial Security Program.

5. The Industrial Security Manual for Safeguarding Classified Information (DOD 5220.22-M), Section III, as it relates to the responsibilities of non-Government organizations and/or individuals for obtaining and maintaining facility and personnel security clearances through the Defense Industrial Security Program operated by the United States Department of Defense.

6. Industrial Security Agreement between the Defense Supply Agency and the U.S. Department of State, letter dated 03/07/69.

7. Additional authorities relevant to this chapter are cited in Chapter 1.

2B. Purpose

This chapter sets forth policy, fixes responsibility, and prescribes procedures for the development, operation and maintenance of the AID Contractor Security Clearance Program and AID Industrial Security Program. The AID Industrial Security Program is designed to provide for the protection of classified information and material, limited official use information and material, the resources of Government information technology systems, and Government objectives and assets, whenever each and/or any of these critical items are subject to being accessed or affected by non-Government organizations and/or individuals.

2C. Background

The expedient exercise of Government functions requires the purchase of goods and/or services from non-Government organizations and/or individuals. Such purchases frequently require access to classified information and material, limited official use information and material, the resources of an information technology system, and/or Government objectives and assets, by non-Government organizations and/or individuals.

2D. Definitions

1. Contract

A mutually binding legal relationship that obligates the seller to furnish certain goods and/or services (including construction) and obligates the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of funds.

2. Contractor

The seller of the goods and/or services. It includes both organizations and individuals.

3. Contractor Employee

An individual employed by a contractor who will be directly involved in the performance of the contract.

4. Facility Security Clearance

An administrative determination by the Department of Defense (DOD) that the contractor (organization, firm, etc.) is eligible for access to classified information and material necessary for performance of a contract. The actual level of a facility security clearance is usually expressed with the level of clearance granted; i.e., top secret, secret, confidential facility security clearance.

5. Nonpersonal Services Contract

A service contract under which personnel rendering the services are not subject, either by the contract's terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the Government and its direct-hire employees.

2D

6. Personal Services Contract

A service contract that, either by the contract's terms or by the manner of its administration, makes the personnel rendering the services appear, in effect, to be U.S. Government employees.

7. Personnel Security Clearance

An administrative determination by IG/SEC or DOD that an individual contractor or contractor employee is eligible for access to classified information and material when necessary for the performance of contractually specified duties, tasks and functions. When a security clearance is issued by the Defense Industrial Security Clearance Office (DISCO), it is routinely referred to as a DISCO clearance.

8. Sensitive Contract

Any contract which requires that the contractor and/or contractor employees to:

a. have access to classified information and material,

b. have access to limited official use (LOU) information and material,

c. have access to any resources of an information technology system,

d. provide any equipment, supplies, and/or materials of a sensitive nature (information technology hardware and/or software, security equipment, communications equipment, etc.), or

e. perform any duties, tasks, or functions that may otherwise fall within the definition of sensitive position provided in Chapter 1.

9. Services Contract

A contract that directly engages the time and effort of a contractor or contractor employee whose primary purpose is to perform an identifiable task rather than furnish a product.

10. Subcontractor

Any supplier, distributor, vendor, or firm that furnishes goods or services to, or for, a prime contractor or another subcontractor.

2D

11. Subcontractor Employee

An individual employed by a subcontractor who is directly involved in the performance of a contract.

12. Access

The ability and opportunity to obtain knowledge of classified or LOU information to operate an information technology system.

13. Additional Definitions

Other terms relevant to this Chapter are defined in Chapter 1

2E. Scope

The policies, procedures and responsibilities set forth in this chapter are applicable to all AID - financed contracts and direct-hire Government personnel involved in the approval, execution, operation or management of such contracts.

2F. Policies

1. General Contract Security Policy

a. Contract Security

No contractor or contractor employee shall be awarded a contract, permitted to provide goods and/or services under a contract, or be retained under a contract unless such an action is clearly consistent with the interests of national security and AID goals.

b. Contractor Personnel Security

The requirements of the Federal Personnel Manual, Section 732, as they relate to the implementation of a personnel security program for Government civilian employment, shall be applied to all contractor personnel except where otherwise specified in this Chapter.

2. Designation and Certification of Contracts

All contracts let for bid shall be designated according to their security sensitivity: a) special-sensitive--special compartmented information, b) critical-sensitive--top secret, c) noncritical-sensitive--secret), and d) nonsensitive--no-access by the applicable contracting officer.

2F

3. Mandatory Security Clauses for Sensitive Contracts

All sensitive contracts or contract modifications that are issued, approved, executed, and/or awarded shall contain the appropriate clause(s) setting forth security-related conditions and/or requirements.

4. Access to Classified Information by Contractor Organizations

a. U.S. Contractor Organizations and Personnel

(1) Classified information and material may be furnished only to U.S. contractor and/or subcontractor organizations that hold a valid facility security clearance, have a need-to-know, and have the capability of safeguarding the information and material in accordance with the provisions of the DOD Industrial Security Program.

(2) Classified information and material may be furnished only to U.S. citizen contractor personnel who hold a valid contractor personnel security clearance.

b. Non-U.S. Contractor Organizations and Personnel

A non-U.S. citizen contractor employee may not occupy a position which requires knowledge of or access to classified information. Although an immigrant alien is eligible for access to classified information under the provisions of the DOD Industrial Security Program, AID has determined that no alien is eligible for access to classified information in any AID - financed program.

5. Access to Limited Official Use Information by Contractor Personnel

a. U.S. Contractor Personnel

Access to LOU information, information technology systems, or permission to perform duties, tasks, and functions designated LOU, may be granted to U.S. citizen contractor personnel provided they have been cleared in accordance with the provisions described in 2H.

b. Non-U.S. Citizen Contractor Personnel Overseas

Under special conditions, Non-U.S. citizen contractor personnel may be granted LOU access. Prior to being granted LOU access, the specific requirement must be defined in writing by the AID official initiating the request. Following Regional Security Officer consultation and concurrence, an investigation is required. The USAID

is responsible for obtaining necessary data for transmittal to the RSO for the investigative effort. Upon completion of the investigative effort, the RSO will submit the investigative report and accompanying recommendations to the USAID Director for final determination.

6. Prohibition of Issuance of Contract Without Security Clearance

Whenever a contractor or subcontractor requires a security clearance for performance of the contract, the required clearance must be in place prior to the issuance of the contract.

7. Revalidation of Security Clearance Prior to the Commencement of Work

No contractor or subcontractor may commence work under an AID contract requiring a security clearance until the contractor's or subcontractor's security clearance has been issued or revalidated in accordance with the provisions of 2H and 2I. In the event that an unclassified contract must be modified to include access to classified or administratively controlled materials, access may not be granted to contractor personnel until such time as their clearances are finalized.

2G. Security Clearance Forms

The following forms, available from the AID Personal Property Management Branch (M/SER/MO/RM/PPM), are required to process a security clearance:

AID 6-10 Request for Clearance (original)

AID 6-85 Foreign Residence Data (original + one)

AID 6-97 Security Acknowledgement (Executed after LOU access is granted and prior to access to LOU material)

AID 6-98 Separation Statement (Executed at termination of LOU access)

AID 610-14 Authority for Release of Information (original + one)

AID 1420-17 Contract Employee Biographical Data Sheet (in addition to SF 86, original + one)

DD-254 Contract Security Classification Specification (Executed when clearance of a firm is required. Original + one)

FD-258 Fingerprint Chart (two originals)

2G

OF-174 Application for employment in the Foreign Services of the United States (original + one)

SF 86 Security Investigation Data for Sensitive Position (original + one)

2H. Clearance Procedures and Responsibilities

1. U.S. Contractors (Firms - Organizations)

a. Classified information may be furnished only to a U.S. contractor or subcontractor who has a valid facility security clearance, a need-to-know, and the capability of safeguarding the information in accordance with the provisions of the DOD Industrial Security Manual. Clearance of U.S. contractors is also required by IG/SEC when access to LOU material is necessary.

b. The Bureau, Office or USAID responsible for executing or approving the AID contract will submit a form AID 6-10, Request for Clearance. Section C, Facility Clearance, on form AID 6-10 will be executed when access to classified information is necessary. Section B, Contractor Clearance, must be executed if access to LOU material, a reputation/integrity check, or a sensitive-no-access clearance is necessary. (Section A is reserved for individuals.)

c. Upon receipt of a request for access to classified information, IG/SEC will determine through the appropriate Defense Contract Administration Services Region (DCASR) whether the contractor has the required facility clearance and/or safeguarding ability. If a clearance is verified, the requesting Bureau, Office or USAID will be notified. If no clearance exists, IG/SEC will facilitate a request for the required clearance through the appropriate DCASR. The Bureau, Office or USAID shall be notified when the clearance is obtained.

d. In those instances where the suitability or reputation of a cleared contractor is in question, IG/SEC will initiate appropriate inquiries to resolve those issues. Section B, of the AID 6-10, Contractor Clearance, should be annotated to facilitate the inquiry when suspicions are raised by the contracting Bureau, Office or USAID.

e. IG/SEC will conduct appropriate inquiries and inform the requesting Bureau, Office or USAID of the results.

f. A clearance by IG/SEC expires at the end of the contract or a period not to exceed five years. Any service beyond that time requires revalidation of the clearance by IG/SEC.

2. Foreign Service National (FSN) and Third Country National (TCN)Contractors

a. FSN and TCN contractors may not occupy a position which requires access to classified information (i.e. national security information). Clearance of FSN and TCN contractors and employees for access to sensitive, unclassified contracts, is the responsibility of the USAID in whose jurisdiction the contract is to be performed.

b. The Department of State, through the Diplomatic Security Service (DSS), investigates and certifies alien applicants and employees in AID overseas posts. USAIDs will determine the need for clearances in consultation with the RSO of the Diplomatic Mission. If a clearance is required for LOU access, the USAID will be responsible for obtaining the necessary data for transmittal to the RSO for processing. The RSO will submit a report and recommendation to the USAID for clearance determination. A list of those employees with LOU access, with appropriate justification for the access, will be submitted by all USAIDs to IG/SEC no later than December 31 of each year.

3. U.S. Personal Services Contractors

a. A personnel security investigation is required for all U.S. citizens entering into AID personal services contracts. The level of sensitivity will determine the scope of the investigation, but at a minimum, a National Agency Check and Inquiries (NACI) must be conducted prior to issuance of the contract.

b. The Bureau, Office or USAID responsible for executing the contract will submit the AID Form 6-10 and accompanying documentation to IG/SEC for processing.

c. When access to classified information is requested, a written justification by the senior AID official must be submitted to IG/SEC. The written justification must state the contractor access requirements and identify the specific materials to which the contractor will require access. IG/SEC will hold final clearance action in abeyance pending the receipt of the justification.

d. After the security forms have been received, IG/SEC will conduct an appropriate investigation, evaluate the findings, note the results on the appropriate copy of the AID 6-10 and forward it to the Bureau, Office or USAID concerned. Failure to enter on duty within 90 days after issuance of the clearance automatically invalidates the clearance and requires revalidation by IG/SEC. An IG/SEC clearance normally expires at the end of the contract or a period not to exceed five years. The five year period presupposes that there is no break in service greater than 90 days. Any service beyond the five year limit requires IG/SEC revalidation.

4. U.S. Nonpersonal Services Contractors

U. S. citizens entering into nonpersonal services contracts require clearance by IG/SEC when access to LOU or classified information is required, when the position is otherwise considered sensitive (Chapter 1), or the contractor is assigned to an ADP-computer position or works in AID offices. The Bureau, Office or USAID responsible for executing the contract must submit the required security forms to IG/SEC in accordance with the provisions of 2G.

5. Restrictions - Marriage to non-U.S. Citizen

a. Any U.S. citizen employee of a contractor or any personal services contractor requiring access to classified information and who is married to a non-U.S. citizen, may not be given access to classified information until appropriate security checks have been made on the employee's spouse. If the contract will be performed in the spouse's country of origin, or former nationality, restrictions may be placed by IG/SEC on the employee's access to classified material. A request for security clearance must include a completed OF-174, (formerly DSP 33) "Application for Employment in the Foreign Service of the United States", completed by the alien spouse, and a written assessment by the senior AID official regarding the impact the marriage might have on the national security.

b. Revalidation of an AID personnel security clearance is also necessary when a previously cleared contractor employee or personal services contractor contemplates marriage to an alien after his/her clearance has been granted and before the contract is completed. A request for such revalidation is submitted to IG/SEC on form AID 6-10 accompanied by OF 174 completed by the intended spouse. A written assessment by the senior AID official regarding the impact the marriage might have on the national security must accompany the request.

2H5

c. IG/SEC may also place restrictions on access to classified material by a contractor employee or a personal services contractor when:

(1) the spouse is employed by a foreign government or foreign entity, or

(2) the contractor employee is a naturalized U.S. citizen and the contract will be performed in his or her country of origin.

d. Any request for relief from these restrictions must be documented fully and subsequently approved by IG/SEC.

2I. Revalidation or Extension of Clearances

1. Revalidation requests are initiated by the interested Bureau, Office or USAID when the contract must be extended. The request shall be submitted to IG/SEC on form AID 6-10, accompanied by an updated SF 86, setting forth all pertinent changes since the last AID clearance, AID 610-14, and FD 258.

2. A revalidation or extension may be requested by cable, with a follow up of all required security forms. The cable request must include full name (no nicknames unless they are so identified). If the person uses only an initial, this must be indicated by providing the initial and followed by (I.O.). The date and place of birth, social security number, citizenship and overseas residences (locations and inclusive dates) must be provided in the cable.

2J. Reinvestigations For Changes In Position Sensitivity

1. All contractor employees selected for moving to a position which is at a higher sensitivity designation than that previously occupied must meet the investigative requirements of the new sensitivity level.

2. If the sensitivity of the position itself is changed, the incumbent may remain in the position, but the investigation required by the new sensitivity must be initiated within seven (7) days after redesignation.

3. If a contractor employee received the required investigation for placement in the new position or in the new sensitivity category, no reinvestigation is required unless updating is necessary.

2K. Adverse Action Procedures

The Industrial Security Regulation DOD 5220.22-R sets forth the procedures for the denial, suspension, or revocation of facility and/or personnel security clearances within the Defense Industrial Security Program.

When contractor clearance actions are being processed under the auspices of IG/SEC, the provisions outlined in 1M apply.

1. Suitability Information

When information is developed during an investigation, which casts serious doubt on the suitability of a contractor, the following procedures shall apply:

a. IG/SEC will inform the appropriate Bureau, Office or USAID and make available appropriate investigative data.

b. The final determination is the responsibility of the appropriate Bureau, Office or USAID.

c. Bureaus, Offices and USAIDs must notify IG/SEC in writing of their decisions so that the clearance action may be finalized.

2L. Security Briefing And Termination Statements

The requesting Bureau, Office or USAID must insure that personal services contractors and contractor employees who are cleared for access to classified or LOU information and material are given a security briefing. Personal services contractors (PSC) cleared for access to LOU information are required to promptly execute form AID 6-97, "Security Acknowledgement", at the beginning of the contract and form AID 6-98, "Separation Statement", at its termination. The originals of AID 6-97 and AID 6-98 must be forwarded to IG/SEC for retention in the PSCs' security files. Contractors cleared for access to classified information must also execute SF 312 "Classified Information Non-Disclosure Agreement." The original of the SF 312 must be forwarded to IG/SEC for retention. Upon separation from the contract, The "Security Debriefing Acknowledgement Statement" on the SF 312 must be executed and forwarded to IG/SEC.

2M. Exceptions

1. Interagency Transfer of Security Clearances and Investigations

Notwithstanding the provisions of 2H, IG/SEC may accept from another federal department (e.g., Department of Defense) the investigative findings and/or security clearances issued by that department pertaining to an AID contractor employee or applicant, and may subsequently issue the appropriate AID security clearance without further investigation.

2. Waiver of Preappointment Investigative Requirement

All requests for waivers to permit personal services contractors and contractor employees to enter on duty pending completion of the appropriate investigation must be submitted by the senior AID official of the Bureau, Office, or USAID with sufficient information and justification to support a finding that the accelerated employment is necessary in the national interest. The waiver request must be sent to IG/SEC for concurrence.

Upon initial assignment of the contractor employee to AID, forms AID 6-10, FD-258, SF 86, AID 610-14, and AID 1420-17 will be completed and forwarded to IG/SEC. In addition, the individual will receive a security briefing by the Unit Security Officer. Failure to complete and submit the required forms will be cause for immediate removal of the contractor employee from all facets of the contract.

TAB II - INFORMATION
SECURITY PROGRAM

TAB 2

INFORMATION SECURITY PROGRAM

This part establishes policy, procedures, and assigns responsibility for the AID Information Security Program. This program is based upon national policy contained in Executive Order 12356, "National Security Information", and assigns procedural responsibility at every level of the organization. Information security is generally associated with national security or classified information, and is concerned with every aspect of proper handling, transmission, storage and safeguarding of national security information. Included within this Part is a position list of Authorized Classification Authorities within AID.

TABLE OF CONTENTS

Chapter 3 - Information Security Program

Chapter 4 - Reserved

CHAPTER 3

INFORMATION SECURITY PROGRAM

3A. Authorities

1. The Inspector General Act of 1978 as amended (P.L. 96-533 and P.L. 97-113)

2. Executive Order 12356, "National Security Information," April 6, 1982

3. Information Security Oversight Office (ISOO) Directive # 1, June 25, 1982

4. Uniform Security Regulations (5 FAM 900), September 1985

3B. Purpose

Part II establishes policy and defines related implementation responsibilities within AID. It supports national security objectives and AID interests through the establishment of administrative and procedural guidelines which ensure an effective Information Security Program.

3C. Policy

1. All employees or associates of AID who are granted access to National Security Information known as Confidential, Secret, Top Secret or administratively controlled information known as Limited Official Use (LOU) must protect this information in accordance with the cited authorities.

2. All new employees and cleared associates of AID must receive an initial security orientation briefing within the first week of duty. Periodic refresher briefings must be provided to all cleared personnel on a bi-annual basis.

3. The head of each major organizational component within AID/W (Bureau/Office,) must formally appoint an individual to serve as the organization's principal point of contact and responsible action officer for administrative security matters. This person, designated as the "Principal Security Officer", (PSO), must be identified to IG/SEC in writing. Subordinate "Unit Security Officers," (USOs) may also be appointed to support the PSO in the administration of security matters. USOs must also be identified to IG/SEC in writing.

3D. Responsibilities

1. General Overview

a. The determination to classify requires specific subject matter expertise, familiarity with classification standards, and an evaluation of the information's impact upon our national security. Typically, the decision to classify rests with a non-Office of Security action officer. While IG/SEC can provide technical assistance concerning classification matters, the effectiveness of the program is heavily dependent upon the knowledge and cooperation of AID non-security personnel.

b. The Office of Security has a program management and an inspection-for-compliance role within the information security arena. The Office of Security monitors national security policies, implements training programs, and coordinates with management personnel to facilitate the establishment of an infrastructure to support organizational compliance.

2. Information Security Briefings

a. All cleared personnel are accountable for ensuring that the sensitive information they possess is handled and protected within established guidelines. Concurrently, it is the responsibility of AID to ensure that cleared personnel are properly briefed regarding these requirements and their responsibilities.

b. All persons cleared for access to national security information or administratively controlled information must attend an information security briefing prior to receipt of classified information and within one week following their arrival for duty. As a minimum, the briefing will: (a) define the terms Top Secret, Secret, Confidential and Limited Official Use, (b) establish the proper handling, storage, marking and classification procedures, (c) define the principle of "Need to Know", and (d) identify appropriate reporting procedures in the event of a possible compromise of classified information, or contact by a representative from one of the criteria countries. All AID/W employees cleared for access to classified material will sign Standard Form 312 during their orientation training. Contractors cleared for access to LOU are required to sign AID 6-9.

c. Personnel overseas shall be briefed by the local Regional Security Officer or the USAID Unit Security Officer. Certification of attendance at this initial security orientation and completed SF 312s must be provided to IG/SEC.

3D2

d. Periodic information security refresher briefings must be provided to each cleared employee or associate of AID on a bi-annual basis. For purposes of consistency throughout AID, briefings should be scheduled during the third quarter of even number years. Personnel not briefed in AID/W by IG/SEC must be briefed at post. AID Unit Security Officers may either present the briefing or request assistance from the Regional Security Officer. Certification of attendance should be forwarded to IG/SEC for inclusion in the individual's security file. As a minimum, the briefing should include: (a) reporting of contacts by criteria country personnel, (b) classification procedures, (c) procedural security, and (d) factors unique to local conditions.

e. Security debriefings must be conducted for all cleared personnel separating from AID. All AID/W debriefings will be conducted by IG/SEC during the separation process. Overseas, security debriefings may be performed in accordance with local policy by either the Regional Security Officer or the USAID Unit Security Officer. A Security Debriefing Statement (SF 312) must be executed and returned to IG/SEC for inclusion within the individual's security file. Contractors cleared for LOU access shall be debriefed; AID Form 6-98 shall be used to document the debriefing. In addition to the subject matter contained on the Debriefing Acknowledgement Statement, the debriefing should provide the separating party with the opportunity to comment upon any personal experiences or facets of security operations which have given cause for concern or need improvement.

3. Security Violation Program

a. In AID/W, IG/SEC will cause after-hours security inspections to be conducted in AID spaces. Classified/LOU materials discovered during an after-hours security inspection will be held by IG/SEC. Upon annotation of logs, the material will be delivered to the Principal Security Officer servicing the organization in which the violation was discovered. The Principal Security Officer must ensure that an OF 118, Report of Security Violation, is completed and forwarded to IG/SEC within ten working days.

b. Overseas, after-hours inspections of AID facilities will be conducted on behalf of IG/SEC by the local RSO. These inspections will be conducted in accordance with local policies. OF-118's will be completed by local security personnel and forwarded to IG/SEC via DS/PI/PRD.

c. In the event of probable compromise of classified or LOU

3D3

information, a security investigation must be conducted by a professional security officer to determine the circumstances surrounding the incident, affix responsibility for the action, and assess potential damage to the national security.

d. The Principal Security Officer, or Unit Security Officer acting in his/her behalf, will conduct the initial investigations on all administrative type security violations. Security violations involving Top Secret or Special Access Program materials and all violations involving a high probability of compromise must be brought to IG/SEC's immediate attention.

e. Within AID/W, the OF 118 Record of Violation must be processed through the Principal Security Officer and forwarded to IG/SEC within three work days of the security violation.

f. Overseas, OF 118 Record of Violation reports must be forwarded through the Regional Security Officer.

g. Responsibility for adjudicating AID security violations rests with IG/SEC. If appropriate, recommendations for disciplinary action may be forwarded by IG/SEC to the Director of Personnel. A courtesy copy of all IG/SEC generated correspondence concerning the results of the adjudication effort, or recommendations for disciplinary action, will be provided to the appropriate executive office or management official.

4. Classified Documents Center

a. The AID Classified Documents Center (CDC) is responsible for conducting reviews of classified documents to determine compliance with the provisions of E.O. 12356. Areas reviewed include determining: (a) whether the information has been properly classified, (b) whether the classifying officer has the appropriate classification authority, and (c) whether the appropriate downgrading and declassification markings have been applied. Unless significant deficiencies impacting upon national security are noted, the results of the CDC review are held by the CDC and used in conjunction with periodic inspections conducted in AID/W and overseas by IG/SEC representatives. CDC documents are also made available to representatives from the General Services Administration's (GSA) Information Security Oversight Office (ISOO) during their inspection of AID. The results of both the IG/SEC and ISOO inspections are presented to the appropriate management official for appropriate action.

3D4

b. Except for documents covered by the provision of 1D4d, copies of all Top Secret, Secret, and Confidential documents must be submitted to the CDC for review. Limited Official Use (LOU) is an administrative control designation, not a security classification, and therefore exempt from CDC review.

c. A copy of all classified cable traffic between AID/W and posts overseas must be forwarded to the CDC by the AID/W Communications Program Management Division of the Office of Management Operations (M/SER/MO/CPM). Cable traffic between posts, which exclude distribution to AID/W, must be forwarded to the CDC. In such an instance, it is the responsibility of the official approving the classification of the message to forward a copy to the CDC. It is also the responsibility of the official authorized to assign a security classification to non-cable correspondence, to forward a copy of the document to the CDC.

d. For classified documents considered by the classification authority to be too sensitive for release outside of action office channels, the classifying authority must submit a Classified Document Index Card, (Form AID 630-2) to the CDC. The official file copy of the document maintained by the originating office must be noted to reflect that a copy of the Form AID 630-2 has been forwarded to the CDC. The official file copy and the copy sent to the CDC must also contain a complete distribution list that includes the names of all recipients, their office symbols, and the number and location of copies.

e. Instructions for completing form AID 630-2, Classified Document Index Card:

(1) Item 1. Authorized Classifier's Name: Enter name of individual authorizing the classification of the document.

(2) Item 2. Originating Office: If Mission or field office, enter office symbol and country name; if AID/W enter office symbol.

(3) Item 3. Subject Title of Document: Enter descriptive phrase that identifies material contained in the document; i.e., names of events, persons, or conditions covered.

(4) Item 4. Distribution: List names of recipients with number of copies sent and location, by office symbol, by Mission or by agency name for distribution outside of AID. Include all file copies.

3D4e

(5) Item 5. Geographic Area Discussed: Enter name of country involved in subject matter of document. If more than one country is involved, list all countries by name in item 14.

(6) Item 6. Document Date: Enter date of document.

(7) Item 7. Document Number or File Code: If telegram, enter message reference number; if other document, enter subject file code assigned in accordance with Handbook 21.

(8) Item 8. Classification Category: Using highest classification assigned to material in the document, enter a check mark in the appropriate box.

(9) Item 9. Declassification Schedule: Leave Blank

(10) Item 10. Exemption Category: Leave Blank

(11) Item 11. Declassification Date: Enter a specific date if known.

(12) Item 12. Declassification Event: If a specific date cannot be identified in item 11, enter an event that will allow for declassification.

(13) Item 13. Preservation Criteria: Indicate whether the document meets AID preservation criteria.

(14) Item 14. Comments: Use this space for a list of country names for item 5, or any other information that may be of assistance in the document review process.

f. Copies of classified documents sent to the CDC must be transmitted in accordance with the transmittal instructions for classified materials, found in the Uniform Security Regulations (5 FAM 900.) Materials shall be forwarded to:

Classified Document Center
IG/SEC/PSI
RM 415, SA 16
AID/W

3D4f

g. M/SER/MO is responsible for conducting a systematic review for declassification. The Records Management Branch, Policy and Analysis Division (M/SER/MO/PA/RM) will provide an annual summary of all documents declassified during the fiscal year. The summary must be provided to IG/SEC within 30 days following the end of each fiscal year.

5. Principal Security Officers

a. As noted in Section 1D1, the proper protection of sensitive information within AID requires a coordinated effort that crosses traditional organization lines. The Office of Security interprets national guidelines, establishes policies, and inspects for program compliance. The heads of major functional areas are responsible for ensuring that appropriate procedures and support personnel are in place to achieve an effective information security program.

b. To facilitate 1D5a, each head of a major functional area must appoint a Principal Security Officer (PSO). The PSO should be at a sufficient grade and operational level to be able to influence Bureau/Office policies and enforce information security program requirements. (Note: The term "Unit Security Officer" overseas and the PSO in AID/W are used synonymously. Moreover, duties and responsibilities described herein are the same.)

c. The PSO will serve as the principal interface between the Office of Security and the Bureau/Office for all administrative security matters. PSOs are required to be sufficiently knowledgeable of security regulations and procedures to serve as the staff advisor on implementation of the information security program. Other PSO responsibilities include distributing security educational materials provided by IG/SEC, ensuring after-duty-hour double checks are conducted in areas where classified materials are handled, coordinating the Bureau/Office security violation program with IG/SEC, establishing and forwarding to IG/SEC a listing of Unit Security Officers (USO) of sufficient grade and position to assist in the administration of the security information program.

d. Unit Security Officer functions are the same as the PSO, except that they are performed at a lower organizational level and do not require further delegation of responsibilities.

6. Original Classification Authority

a. Authority to originally classify information within AID must be specifically delegated by the Administrator. Authority rests within

the position, not the individual. The Office of the Executive Secretariat will provide, for distribution throughout AID, a listing of positions whose incumbents are authorized to originally classify. This listing will be published on an annual basis, with updates as appropriate.

b. Each cleared employee within AID has the authority to derivatively classify information.

7. Funding for Security Information Program Equipment

a. With the exception of the Office of the Inspector General, the funding and procurement of all security equipment (security containers, barlock cabinets, padlocks, shredders) and services associated with the protection of national security information within AID/Washington is the responsibility of M/SER/MO. The Office of the Inspector General may fund directly, or reimburse AID for services rendered.

b. Overseas, procurement and servicing of equipment associated with the protection of classified information is a USAID responsibility.

8. AID Security Forms

The following security forms associated with the Information Security Program will be acquired and used throughout AID:

a. SF 700, Security Container Information, NSN 7540-01-214-5372

This form must be attached to the inside of any container used to store classified information. This is a two-part form, Part 1 identifies persons responsible for the container; Part 2 contains the combination (see 5 FAM 900 for disposition). In AID/W, a copy of Part 2 must be sent to IG/SEC. Part 2 must be protected in the same manner as the highest level of classified material stored within the container. Overseas, a copy should be retained in accordance with local post policies.

b. SF 701, Activity Security Checklist, NSN 7540-01-213-7899

This form must be used by all offices for after-duty-hours security checks.

3D8

c. SF 702, Security Container Check Sheet, NSN 7540-01-213-7900

This form must be placed on the outside of any security container that is used to store classified information. It must be initialed by whomever opens or closes the container and by the after duty-hours checker.

d. SF 703, TOP SECRET Cover Sheet, NSN 7540-01-213-7901

This form must be affixed to each Top Secret document when the document is not stored in a security container.

e. SF 704, SECRET Cover Sheet, NSN 7540-01-213-7902

This form must be affixed to each Secret document when the document is not stored in a security container.

f. SF 705, CONFIDENTIAL Cover Sheet, NSN 7540-01-213-7903

This form must be affixed to each Confidential document when the document is not stored in a security container.

g. AID 630-2, CLASSIFIED Document Index Card

This form must be used when classified documents are considered too sensitive to be forwarded to the CDC.

Attachment 3A Positions within AID in which the incumbents have original Secret classification authority

Attachment 3B Positions within AID in which the incumbents have original Confidential classification authority

Attachment 3C Positions within AID in which the incumbents have declassification authority

ATTACHMENT 3A

AID ORIGINAL SECRET CLASSIFICATION AUTHORITIES

Office of the Administrator (A/AID)

Administrator
Deputy Administrator
Counselor
Director, Task Force on Humanitarian Aid for Central America (TFHA)

Office of the Executive Secretary (ES)

Executive Secretary

Bureau for Program and Policy Coordination (PPC)

Assistant Administrator
U.S. Representative to the Development Assistance Committee
Development Coordination Officer, Food and Agriculture Officer

Bureau for Science and Technology (S&T)

Senior Assistant Administrator

Bureau for Personnel and Financial Management (PFM)

Assistant Administrator

Bureau for Asia and Near East (ANE)

Assistant Administrator
Deputy Assistant Administrator
Deputy Assistant Administrator

Bureau for Latin America and the Caribbean (LAC)

Assistant Administrator
Deputy Assistant Administrator

Bureau for Africa

Assistant Administrator
Deputy Assistant Administrator
Deputy Assistant Administrator

Bureau for Private Enterprise (PRE)

Assistant Administrator

Bureau for Food for Peace and Voluntary Assistance (FVA)

Assistant Administrator

Office of Legislative Affairs (LEG)

Director

Office of the Inspector General (IG)

Inspector General
Deputy Inspector General/Assistant Inspector General for Audit
Counsel to the Inspector General
Assistant Inspector General for Investigations
Assistant Inspector General for Security

Office of U.S. Foreign Disaster Assistance (OFDA)

Director

Office of the Science Advisor (SCI)

Science Advisor

Asia and Near East

Bangladesh	Mission Director
Burma	AID Representative
Egypt	Mission Director
Fiji	Regional Director, South Pacific
India	Mission Director
Indonesia	Mission Director
Italy	FAO Affairs Officer, Rome
Jordan	Mission Director
Lebanon	AID Representative
Morocco	Mission Director
Nepal	Mission Director
Oman	AID Representative
Pakistan	Mission Director
Philippines	Mission Director
Sri Lanka	Mission Director
Thailand	Mission Director

Tunisia	Mission Director
Yemen	Mission Director

Latin America and the Caribbean

Barbados	Regional Director, Caribbean
Belize	AID Representative
Bolivia	Mission Director
Brazil	AID Representative
Colombia	AID Representative
Costa Rica	Mission Director
Dominican Republic	Mission Director
Ecuador	Mission Director
El Salvador	Mission Director
Guatemala	Mission Director
Haiti	Mission Director
Honduras	Mission Director
Jamaica	Mission Director
Mexico	AID Representative
Peru	Mission Director
Uruguay	AID Representative

Africa

Botswana	Mission Director
Burkina Faso	Mission Director
Burundi	AID Representative
Cameroon	Mission Director
Cape Verde	AID Representative
Chad	AID Representative
Ethiopia	AID Representative
Gambia	AID Representative
Ghana	AID Representative
Guinea	Mission Director
Guinea-Bissau	AID Representative
Ivory Coast	Regional Director, West & Central Africa
Kenya	Mission Director
	Regional Director, East & Southern Africa
Lesotho	Mission Director
Liberia	Mission Director
Madagascar	Mission Director
Malawi	Mission Director
Mali	Mission Director
Mauritania	AID Representative
Mozambique	Mission Director
Niger	Mission Director

Nigeria	AID Affairs Officer
Rwanda	Mission Director
Senegal	Mission Director
Somalia	Mission Director
South Africa	Mission Director
Sudan	Mission Director
Swaziland	Mission Director
Tanzania	Mission Director
Togo	AID Representative
Uganda	Mission Director
Zaire	Mission Director
Zambia	Mission Director
Zimbabwe	Mission Director

ATTACHMENT 3B

AID ORIGINAL CONFIDENTIAL CLASSIFICATION AUTHORITIES

Regional Inspectors General for Audit and Regional Inspectors General for Investigations:

Cairo
Manila
Singapore
Dakar
Nairobi
Tegucigalpa

ATTACHMENT 3C

AID DECLASSIFICATION AUTHORITIES

All individuals with Secret and Confidential original classification authority plus the following:

Office of the Executive Secretary (ES)

Deputy Executive Secretary

Bureau for Program and Policy Coordination (PPC)

Deputy Assistant Administrator
Associate Assistant Administrator, Office of Policy Development and Program Review
Associate Assistant Administrator, Office of Planning and Budget
Associate Assistant Administrator, Center for Development Information and Evaluation
Associate Assistant Administrator, Office of Economic Affairs
Director, Executive Management Staff
Director, Multilateral Financial Institutions Staff
Director, Office of Women in Development
Director, Office of Donor Coordination

Bureau for Science and Technology (S&T)

Deputy Assistant Administrator for Research
Deputy Assistant Administrator for Technical Cooperation
Agency Director, Directorate for Food and Agriculture
Agency Director, Directorate for Energy and Natural Resources
Agency Director, Directorate for Human Resources
Agency Director, Directorate for Health
Agency Director, Directorate for Population
Director, Office of Program
Director, Office of Management
Director, Office of Research and University Relations
Director, Office of Technical Review and Information
Director, Office of Nutrition
Director, Office of Forestry, Environment and Natural Resources
Director, Office of Energy
Director, Office of Rural and Institutional Development
Director, Office of Education
Director, Office of International Training
Chief, Publications and Information Division

Bureau for Management (M)

Assistant Administrator
Deputy Assistant Administrator
Associate Assistant Administrator
Director, Management Support
Director, Office of Procurement
Director, Office of Information Resources Management
Director, Office of Management Operations

BIFAD Support Staff (BIFAD/S)

Executive Director

Bureau for External Affairs (XA)

Assistant Administrator
Deputy Assistant Administrator
Director, Office of Public Liaison
Director, Office of Audio-Visual Production
Director, Office of Public Inquiries
Media Operations Coordinator, Office of Press Relations

Office of Legislative Affairs (LEG)

Deputy Director

Office of Equal Opportunity Program (EOP)

Director

Office of Small and Disadvantaged Business Utilization (OSDBU)

Director

Bureau for Food for Peace and Voluntary Assistance (FVA)

Deputy Assistant Administrator for Food for Peace Coordination
Deputy Assistant Administrator
Director, Office of Program Policy and Management

Bureau for Private Enterprise (PRE)

Deputy Assistant Administrator
Director, Office of Program Review
Director, Office of Project Development

Director, Office of Investment
Director, Office of Housing and Urban Programs
Assistant Director, Shelter and Urban Programs and Policy Division

Bureau for Africa (AFR)

Associate Assistant Administrator, Private Enterprise Staff
Director, Office of Emergency Operations
Director, Office of Management
Director, Office of Development Planning
Director, Office of Project Development
Director, Office of Technical Resources
Director, Office of Eastern Africa Affairs
Director, Office of Central and Coastal Africa Affairs
Director, Office of Sahel and West Africa Affairs
Director, Office of Southern Africa Affairs
Controller

Bureau for Asia and Near East (ANE)

Director, Executive Management Staff
Director, Office of Project Development
Director, Office of Technical Resources
Director, Office of East Asian Affairs
Director, Office of Egyptian Affairs
Director, Office of Middle Eastern, European and North African Affairs

Bureau for Latin America and the Caribbean (LAC)

Associate Assistant Administrator, Office of Central American and Panamanian Affairs
Director, Executive Management Staff
Director, Administration of Justice and Democratic Development Staff
Director, Private Sector Staff
Director, Office of Development Resources
Director, Office of Development Programs
Director, Office of Caribbean Affairs
Director, Office of South American and Mexican Affairs Controller

Office of the General Counsel

Assistant General Counsel for Africa
Assistant General Counsel for Latin America and the Caribbean
Assistant General Counsel for Asia and Near East
Assistant General Counsel for Legislation and Policy
Assistant General Counsel for Employee and Public Affairs
Assistant General Counsel for Central Programs

Assistant General Counsel for Litigation and Enforcement
Assistant General Counsel for Contract and Commodity Management
Assistant General Counsel for Private Enterprise

In the Field

Deputy/Assistant Mission Directors
Program Officers
Deputy Regional Directors
Other positions more senior

CHAPTER 4

RESERVED

TAB III - AID WASHINGTON SECURITY PROGRAM

TAB 3

AID WASHINGTON SECURITY PROGRAM

This part establishes policy, procedures and assigns responsibilities for security issues within AID Washington and the Overseas Private Investment Corporation (OPIC). It is intended to provide uniformity and direction resulting in the protection of AID and OPIC personnel, physical assets and National Security Information.

TABLE OF CONTENTS

Chapter 5 - AID Washington Security Program

Chapter 6 - Reserved

CHAPTER 5

AID WASHINGTON SECURITY PROGRAM

5A. Authorities

1. The Inspector General Act of 1978 as amended (P.L. 96-533 and P.L. 97-113)

2. Executive Order 12356, "National Security Information," April 6, 1982

3. Uniform Security Regulations (5 FAM 900), September 1985

5B. Purpose

Part III establishes responsibilities, procedures, operational control and budgeting offices for the AID Washington security program.

5C. Scope

The policies, responsibilities and procedures set forth in this chapter are applicable for all AID personnel and facilities within the Washington, D.C. area.

5D. Responsibilities

1. The Inspector General Act, as amended states, "...the Inspector General of the Agency for International Development -- (1) shall supervise, direct, and control all security activities relating to the programs and operations of that Agency, subject to the supervision of the Administrator of that Agency;..."

2. With the exception of the Office of the Inspector General, M/SER/MO is responsible for: (a) funding and acquisition of office space, support services and equipment, (b) issues of public safety and (c) all AID/W costs associated with security.

3. In the event of differences between the Office of the Inspector General and AID management concerning what constitutes reasonable levels of protection, the issue shall be resolved by the AID Administrator.

5E. Policy

AID/W management, in concert with IG/SEC, shall develop, install and maintain security procedures and systems that provide adequate levels of protection for AID's classified holdings, personnel and facilities.

5F. Building Security

1. Acquisition of Space

Acquisition of office or warehouse space outside the main Department of State building in Washington shall not occur without the submission of an IG/SEC security survey report to M/SER/MO/RM. IG/SEC must be notified prior to acquisition to ensure that security considerations are addressed in appropriate planning documents. Advance notice of proposed space acquisition will facilitate the security survey and installation of IG/SEC - M/SER/MO agreed upon security measures prior to occupancy.

2. Security Surveys

IG/SEC shall submit updated security surveys of all AID/W properties to M/SER/MO/RM on a bi-annual basis. M/SER/MO/RM will respond to IG/SEC within thirty days of receipt of the survey report concerning planned or completed actions to implement security recommendations.

3. Remedial Security Recommendations

In addition to the bi-annual security survey, IG/SEC may make specific emergency recommendations for corrective action as developments warrant. M/SER/MO/RM should respond to IG/SEC concerning these emergency recommendations, and their intended course of action, within three working days.

4. Alarm Coverage

Requests for new alarm systems or modifications to existing systems shall be submitted by the requesting office to M/SER/MO/RM through IG/SEC. The request for coverage should be in memo format and include a justification for the service. IG/SEC will subsequently conduct a preliminary survey of the area in question and forward the original request, along with the survey results and appropriate recommendations, to M/SER/MO/RM for approval. M/SER/MO/RM will initiate a contract for the service and obligate funds based upon their availability. The final survey for proposed alarm coverage will be provided by the contractor and will be endorsed appropriately by IG/SEC.

5F

5. Guard Service

Requests for guard service will be forwarded to M/SER/MO/RM; a copy should be provided to IG/SEC. A justification and security endorsement must accompany all requests before M/SER/MO/RM will consider them. Based upon M/SER/MO/RM and IG/SEC concurrence, and the availability of funds, the guard service will be contracted for by M/SER/MO/RM. Although M/SER/MO/RM funding will be employed to pay for the contract, a representative from IG/SEC will provide technical assistance to the Contracting Officer's Technical Representative (COTR). The technical assistance will normally include oversight of the guard program and development of guard orders.

5G. Identification Cards

1. Eligibility for an AID ID Card

Receipt of an AID ID card is conditional upon the favorable adjudication of a personnel security investigation by IG/SEC and request for the issuance of a card by a sponsoring AID element. Executive/Management officers in the major organizational components of AID (Bureaus or Offices) are authorized sponsoring officials. ID cards for contractor personnel are subject to the same constraints as direct-hire employees.

2. Degree of Access/Privilege Granted by the ID Card

The card is programmed by an automated access control system used by the Department of State. It is capable of allowing varying degrees of escort privilege and access, dependent upon the level of clearance granted and the requirements of the position occupied by the card holder. Determination of card privileges is the responsibility of the sponsoring official. Employees in critical-sensitive positions will receive type "A" passes allowing escort privileges and 24 hour access to the main Department of State building. Employees in noncritical-sensitive positions will receive type "B" passes, allowing varying levels of access and escort privilege.

3. Procedures For Obtaining ID Card

When the need for an ID card is established, the sponsoring Bureau/Office must prepare the administrative portion of the appropriate AID Form 610-5 (Authorization to Issue Department of State Building Pass A) or AID Form 610-5A (Authorization to Issue Department of State Building Pass B). The sponsoring organization must then forward the 610-5(A) to IG/SEC for clearance verification. Upon verification of the

clearance, the form is returned to the sponsor for issuance to the intended card holder. The prospective card holder may then take the authorization form to the designated ID unit for issuance of the ID card.

4. Employees Returning From Overseas

Employees returning from overseas in need of a new ID card should notify Foreign Service Personnel in advance of their return. Foreign Service Personnel will prepare the appropriate authorization form and forward it to IG/SEC. Upon verification of the clearance by IG/SEC, the form will be returned to Foreign Service Personnel for retention until the employee returns to AID/W. Upon return, the employee may retrieve the form from Foreign Service Personnel and report directly to the ID issuing unit.

5. Expiration Dates

Expiration dates associated with the initial issuance of the new ID cards have been staggered to avoid administrative problems associated with card renewals. For direct-hire employees, subsequent issuance of cards will occur on a five year cycle. Contractor ID cards will coincide with the expiration date of their contract.

6. Loss of ID Card

The Office of Security should be notified immediately by phone or cable when an ID card is lost. This will allow elimination of the card from the computer system and prevent unauthorized access into the main Department of State building. A follow-up memo explaining the circumstances of the loss must be submitted by the card holder. The memo should be submitted through the sponsoring official to IG/SEC and be accompanied, when appropriate, by a new 610-5(A) form.

7. Termination of Employment

Employees and contractors terminating association with AID must surrender their ID cards as part of their separation process. Within AID/W., the cards must be surrendered to IG/SEC. Overseas, the cards may be turned in to the Management or Executive Office where they shall be forwarded to IG/SEC via classified pouch. The cards shall be accompanied with a memo which advises that the individuals have resigned or retired.

5H. AID/W Locks/Combinations

1. Combination Padlocks

Combination padlocks used to secure barlock containers may not be used in all instances for the protection of classified material within AID Washington. It is incumbent upon the holder of classified material to be aware of and comply with the appropriate storage requirements of 5 FAM 900. Combination padlocks may be obtained from M/SER/MO/RM via requisition. Combinations for padlocks must be changed in accordance with the guidance contained in 5 FAM 900. Padlock combinations will be set by the appropriate Principal or Unit Security Officer. Recording of the combinations must be accomplished in accordance with the instructions found on SF 700. A copy of the combination shall be forwarded to IG/SEC via the PSO.

2. Security Container Combination Locks

Built-in combination locks on security containers shall be changed only by representatives from the Office of Security or their designated representative. As with combinations for padlocks, the combination must be recorded on SF 700 and a copy of the combination forwarded through the PSO to IG/SEC.

5I. AID/W. Emergency Situations

1. Bomb Plans

Each AID/W facility must have a current bomb plan. The plan should be incorporated into the public safety contingency plans coordinated by M/SER/MO and codified in AID Handbook 20, Chapter 3, "Safety, Health and Civil Defense Programs." More detailed plans and guidance for responding to bomb threats and other emergencies are provided in the derivative Occupant Emergency Plan prepared for each AID occupied building under the auspices and oversight of the Occupational Safety and Health (OSH) officer in M/SER/MO.

2. Reports of Crimes in Progress

Initial reports of crimes in progress should be made directly to the local police department and the General Services Administration Police. Immediate follow-up reporting should be made to the Office of Security.

5I

3. Emergency Action Directory

Designated points of contact and telephone numbers are listed in Section F, the Emergency Action Directory, of the AID Washington Telephone Directory. All employees should become familiar with the directory.

CHAPTER 6

RESERVED

TAB IV - OVERSEAS
SECURITY PROGRAM

TAB IV

OVERSEAS SECURITY PROGRAM

This part describes the security program requirements which pertain to USAID activities overseas. The goal of this program is to prevent terrorists, criminal, and other hostile groups from causing injuring to AID personnel and to preclude the compromise of national security information. This part also addresses employee responsibilities and procedures to implement the AID overseas security program. The concept of the program is to provide 24-hour protection to personnel assigned overseas. Elements of the program include office building security, armored vehicles, residential security, local guards, and operations security.

TABLE OF CONTENTS

Chapter 7 - Security Responsibilities and Relationships at Overseas Posts
Chapter 8 - USAID Office Building Physical Security
Chapter 9 - Security Procedures
Chapter 10 - Operations Security
Chapter 11 - Security Communications
Chapter 12 - Armored Vehicles
Chapter 13 - Overseas Residential Security
Chapter 14 - Local Guards
Chapter 15 - Construction and Transit Security
Chapter 16 - Reserved

CHAPTER 7

SECURITY RESPONSIBILITIES AND RELATIONSHIPS AT OVERSEAS POSTS

7A. Authorities

1. The Vienna Convention on Diplomatic Relations, adopted at Vienna on 18 April 1961

2. The Inspector General Act of 1978 as amended (P.L. 96-533 and P.L. 97-113)

3. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399) (Diplomatic Security Act)

4. Agency for International Development - Department of State Overseas Security Agreement, December 7, 1987

5. National Security Decision Directive (NSDD) 298, "National Operations Security Program," January 22, 1988

6. Foreign Assistance Act of 1961 as amended (22 USC 2349aa-4)

7B. Purpose

This chapter establishes security program responsibilities for AID personnel and describes security relationships at overseas posts.

7C. Responsibilities

1. Host Government

The host government has the primary responsibility for the protection of United States Government personnel and facilities located within its borders.

2. United States Government

a. The Secretary of State is responsible for providing security for U.S. Government operations of a diplomatic nature. Under the Diplomatic Security Act, these security responsibilities include the protection of all U.S. Government personnel on official duty abroad and their accompanying dependents (except personnel under the command of a U.S. area military commander) and the establishment and operation of security functions at all U.S. missions abroad.

7C2

b. The Inspector General for the Agency for International Development is vested under the Inspector General Act of 1978 (P.L. 96-533 and P.L.97-113) with the responsibility for providing security services to AID. The Assistant Inspector General for Security is directly responsible to the IG and Administrator for implementing the AID security program.

c. The Chief of Mission (COM) is charged by the Secretary of State with the ultimate responsibility at post for the security of facilities and personnel under his control.

d. The Regional Security Officer (RSO) is responsible to the Assistant Secretary for Diplomatic Security and to respective Chiefs of Mission for managing and conducting the Department's overseas security programs. Responsibilities of the RSO are enumerated in Attachment 1A.

e. The senior AID official at post is responsible for implementation of the USAID security program. This includes coordination with the RSO and participation in the post Emergency Action Committee (EAC). The senior AID official shall appoint, in writing, a Unit Security Officer to manage the USAID security program. The USAID USO shall be an AID U.S. direct-hire employee and hold a minimum grade of FS-04. The USAID executive officer or Management Officer is normally appointed as USO.

f. The USAID Unit Security Officer (USO) is responsible to the senior AID official for managing the local USAID security program in accordance with this Handbook and the guidance provided in USO Manuals Number 1 and 2.

g. Each AID employee is responsible for taking reasonable personal security measures when assigned overseas. Those measures should be appropriate to local circumstances including as a minimum, those measures that would be taken to protect themselves, their families, their homes, and other possessions if residing in the United States. An assignment overseas does not absolve the employee of this responsibility.

7D. AID - State Overseas Security Agreement

There is an agreement between AID and the Department of State which sets forth respective responsibilities for the performance of security functions overseas. The text of the agreement is provided in attachment 7A.

ATTACHMENT 7A

THE AGENCY FOR INTERNATIONAL DEVELOPMENT/DEPARTMENT OF STATE OVERSEAS SECURITY AGREEMENT

I. BACKGROUND

A. Under the Inspector General Act of 1978 as amended (P.L. 96-533 and P.L. 97-113), the Inspector General of the Agency for International Development is charged with specific responsibilities for providing security services to that establishment and to the International Development Cooperation Agency. These mandated responsibilities include the supervision, direction, and control of all security activities relating to AID and the I.D.C.A. programs and operations, the performance of inspections, and the preparation of semiannual reports to Congress on said activities.

B. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 assigns responsibility to the Secretary of State to develop and implement, in consultation with the heads of other federal agencies, policies and programs to provide for the protection of all U.S. government personnel on official duty overseas, and the establishment and operation of security functions at all U.S. missions abroad. To facilitate the fulfillment of this responsibility, other federal agencies are therein directed to cooperate and assist the Department of State, through agreement, to the maximum extent possible. The Omnibus Act expressly identifies types of assistance to be rendered, i.e., logistical support and security inspections. It also states that federal agencies may perform other overseas security functions as authorized by the Secretary of State.

II. STATEMENT OF AGREEMENT

A. In accordance with the above legislation and the policies enacted by the Overseas Security Policy Group (O.S.P.G.), the undersigned agree that the Department of State, Bureau of Diplomatic Security (DS) will perform certain overseas security functions for the Agency for International Development, and that the AID Inspector General, Office of Security (IG/SEC) will cooperate and assist the Department to fulfill this responsibility in the manner and to the extent hereinafter set forth. The provisions of this Agreement supersede those contained in the previous Overseas Security Agreement between the Agency for International Development and the Department of State dated August 26, 1968.

B. Nothing in the following agreement shall derogate from or be construed to conflict with the authorities and responsibilities of the Chief of Mission under Section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), or to derogate from or conflict with the responsibility of agencies under section 207 to keep the Chief of Mission fully and currently informed and to ensure that its employees comply with the applicable directives of the Chief of Mission.

III. PHYSICAL SECURITY SERVICES

A. DS will provide to IG/SEC, in a timely manner, information pertinent to AID security. Such information will include, but not be limited to, threat reports and analysis, approved modifications to D.O.S. security standards, and updates on D.O.S.-approved security products, systems or designs.

B. Overseas, the Regional Security Officer (RSO) will advise, through DS, the respective USAID and IG/SEC of any specific threat information concerning USAID facilities or personnel, and specify the security measures taken or planned to counter such threats. The RSO will also inform, through DS, USAID and IG/SEC of any general threat information concerning the U.S. community at post.

C. DS, through the responsible RSO, will provide or direct physical, technical, and procedural security services at all USAID posts overseas.

D. The RSO will conduct, on a regular basis, complete physical, personnel and procedural surveys of USAID missions and facilities. The RSO will coordinate through DS with the responsible IG/SEC Security Regional Operations Officer in advance of the projected USAID survey so that IG/SEC may facilitate and, whenever feasible, participate in the survey. IG/SEC will provide an expeditious response to DS regarding their intent to participate in the survey. New surveys will be conducted according to DS policy or whenever major changes occur in the physical structure, size, or location of space occupied by USAID in separate facilities. These changes may include, but are not limited to, completion of significant physical security improvements, acquisition of additional space in the same building, leasing of additional office space in another building, or relocation of the USAID mission to a new site. Copies of these types of reports will be forwarded to IG/SEC for review/concurrence with report recommendations. Identification of funding will be provided prior to the initiation of any security projects resulting from the recommendations.

E. The RSO will arrange for technical security inspections by appropriate technical security personnel of USAID premises and facilities as required by local conditions, or in response to a specific request from IG/SEC. The RSO will also arrange for technical security systems installation, maintenance and repair as required at USAID facilities.

F. The RSO will manage the guard force assigned to USAID office facilities and residences. Appropriate guard and watchman procedures for the above locations will be established and documented in the form of written guard orders, copies of which will be provided to the USAID Unit Security Officer (USO). Marine security guards will be assigned to USAID facilities when such assignment is deemed to be warranted by DS and IG/SEC, subject to other considerations such as the establishment of positions by the Department of State and the availability of Marine Corps personnel.

G. The RSO will conduct appropriate investigations of all incidents occurring on USAID premises or at USAID residences involving unauthorized or forced entries, physical penetration, and other similar breaches of security, and forward a detailed report of investigation through DS to IG/SEC in a timely manner.

H. IG/SEC will conduct periodic security inspections of USAID office facilities, residences, and warehouses, to evaluate compliance and assist USAID's in developing methods and strategies for meeting DOS and AID security standards and regulations. In support of these inspections, Regional Security Officers, will make available to IG/SEC such locally held files and information pertaining to USAID security as may be required.

I. IG/SEC will administer the AID security radio program in support of all USAID direct-hire and U.S. contractor personnel, regardless of location. The radios provided by IG/SEC will be fully compatible with the Department of State emergency and evacuation system.

IV. PERSONNEL SECURITY SERVICES

A. DS will conduct personnel security investigations, pursuant to Executive Order 10450, of US citizens who have served overseas and are applying for direct-hire and contract positions in AID as may be requested by the Assistant Inspector General for Security (AIG/SEC). When requested by the AIG/SEC, DS will also conduct personnel security investigations of U.S. citizen direct-hire and contract personnel serving overseas.

B. The RSO will screen all USAID alien applicants or personnel for suitability and reliability, and if appropriate, certify them as acceptable for employment. The USAID Unit Security Officer (USO) will assist the RSO or Post Security Officer (PSO) in the conduct of these investigations when so requested. The closest cooperation will be maintained between the RSO and PSO and the USAID USO to facilitate accomplishment of local investigations in the most effective way.

C. The RSO will conduct required investigations for the USAID Mission Director in matters concerning alien contractors and alien contractor personnel.

D. The RSO will conduct investigations on intended alien spouses of USAID's U.S. citizen employees as requested by the Mission Director or IG/SEC.

E. When the RSO receives reports or allegations bearing on the security or loyalty of USAID employees, the RSO shall communicate this information to DS. DS will coordinate matters with the AIG/SEC prior to issuing direction and guidance to the RSO. Except for emergency situations, or at the direction of the COM, the RSO will not initiate a formal investigation without DS approval. This does not preclude the RSO from conducting preliminary inquiries to substantiate allegations.

F. In the event that DS receives reports or allegations reflecting adversely on the suitability of AID U.S. employees overseas, the RSO will immediately communicate this information to IG/SEC, via DS, for determination of investigation requirements.

G. Except for emergency situations, no AID U.S. citizen employee under investigation by the RSO shall be confronted in an interview situation without approval and instruction from IG/SEC through DS.

H. The RSO will provide the IG/SEC, through DS, with detailed reports of all security investigations conducted for AID

I. DS will not undertake any criminal or administrative investigations of AID U.S. direct-hire and contractor employees, or foreign national personnel, unless so requested by the AID Regional Inspector General for Investigations (RIG/II), who has sole responsibility for such investigations. This does not preclude the RSO from conducting preliminary inquiries to substantiate allegations.

The Chief of Mission may authorize investigations of extraordinary circumstances when consideration of mission security or jeopardy to human life do not permit the seeking of prior approval from Agency headquarters.

V. TRAINING SERVICES

A. The USAID Unit Security Officer (USO) will be trained and assisted in security matters by the appropriate Regional or Post Security Officer.

B. The RSO will include AID U.S. direct-hire and U.S. contractor personnel in all security training and indoctrination lectures and provide them with appropriate security briefing materials.

VI. ISSUE RESOLUTION

Should a conflict arise between USAID officials and DS Security Officers concerning the substance or interpretation of security matters, the issues in question will be forwarded to DS and the IG/SEC for resolution.

For the Administrator:

Herbert L. Beckington
Inspector General
Agency for International Development

12/7/87

For the Secretary:

Robert E. Lamb
Assistant Secretary for Diplomatic Security
Department of State

November 15, 1987

CHAPTER 8

USAID OFFICE BUILDING PHYSICAL SECURITY

8A. Authorities

1. AID Physical Security Standards for USAID Office Buildings, dated June 1987 (Appendix B of the AID Unit Security Officer Manual, Book 2).

2. Confidential State Cable 072432, dated March 8, 1988, Subject: Definition of Approved Vaults and Strong Rooms (U).

3. Confidential State Cable 324710, dated October 17, 1987, Subject: New Minimum Overseas Standards for Classified Information (U).

8B. Purpose

This chapter identifies the physical security requirements for USAID office buildings.

8C. Definitions

1. USAID Office Buildings

Any office building containing an area routinely utilized for the conduct of official business. The area must also be routinely occupied by U.S. direct-hire staff.

2. National Security Information

Information classified at the Confidential, Secret, or Top Secret level. The term "classified" does not include Limited Official Use (LOU) information.

8D. Policy

1. A terrorist or mob attack can occur at any time or at any place in the world. AID cannot guarantee the absolute security of personnel assigned abroad. Overseas security measures are designed to provide a relatively secure environment until the host government responds or until U.S. sponsored emergency evacuation occurs.

2. The ability of host governments to protect U.S. personnel varies significantly. When it is determined that the host government is not able or willing to provide the requisite level of assistance, and that

8D2

adequate defensive security measures cannot be implemented, it may be necessary for the U.S. government to consider the withdrawal of U.S. personnel and/or close down the USAID.

3. Adequate security measures for office buildings must be implemented at each USAID post to provide a level of security commensurate with the local threat, in accordance with AID security standards. USAIDs must comply with the security standards which are contained in USO Manual Book 2. Classified material must be stored in accordance with the security standards contained in 2A3 (Confidential 1987 State Cable 324710).

4. To ensure adequate security planning, IG/SEC shall be notified as soon as a USAID identifies a need for new or additional office space. IG/SEC is responsible for funding or providing physical security equipment.

5. All security measures for USAID contractor facilities will be funded through the applicable contract.

8E. Objective

The objective of office building physical security systems and measures is to prevent loss of life caused by explosive effects, protect personnel against violent mobs, terrorists and other intruders, and safeguard national security information.

8F. Physical Security Systems

1. Physical security systems are based on the concept of a layered or tiered system of defenses. These defenses are designed to provide protection by delaying, minimizing, or deterring specific types of threats. The threats to the AID office building are explosive effects, bomb-laden vehicles, violent mobs, terrorists and other intruders.

2. To minimize explosive effects, office buildings must have sufficient structural strength and separation distance (setback) from publicly accessible detonation points. Glass surfaces shall be treated with protective film to minimize the shards resulting from an explosion.

3. To prevent bomb-laden vehicles from forcibly entering a compound, vehicle control barriers (bollards, planters, walls, and other traffic control devices) must be employed.

4. A combination of related security systems have to be employed to prevent violent mobs, terrorists and intruders from entering buildings:

8F4

a. Walls, fences, and/or pedestrian gates must be employed at the perimeter.

b. The entry and exit points (doors) of the building and the building's exterior (walls, grilled windows) need to be of sufficient strength to resist ballistic attack and delay forced entry. The period of delay has to be sufficient to enable personnel to vacate the immediate area and reach a temporary refuge or safely disperse.

c. The public access control (PAC) system must be of sufficient strength to resist ballistic attack and delay forced entry.

d. Walk-through or hand-held metal detectors must be employed to detect weapons.

e. An emergency notification system must be installed, maintained, and periodically tested to inform employees of threatening situations such as bomb threats, terrorist and criminal activity, and fire.

5. A temporary refuge (safehaven) must be incorporated into the building to provide a sufficient level of protection for a period of time to permit a response by the host government. The design of the temporary refuge shall provide for a means of escape from the building in the event of a fire or other life threatening situation. The refuge must contain:

a. Communications equipment for requesting assistance.

b. An alternate means of egress from the building.

c. An ability to destroy all classified holdings. The emergency destruction equipment must connected to a reliable emergency power source.

6. USAIDs certified for overnight storage of national security material will provide a vault or strong room built to the standards contained in 2A2 (Confidential 1988 State Cable 072432).

8G. Accountability, Repair, Maintenance and Replacement

Accountability for physical security equipment provided or funded by IG/SEC rests with the USAID. AID Handbook 23, Support Overseas, applies except that security equipment cannot be disposed locally without IG/SEC authorization. USAIDs have the basic responsibility for repair,

maintenance and replacement of the equipment. IG/SEC will provide information to assist USAIDs with this responsibility. In addition, USAID office buildings are included in the Department's Security Equipment Maintenance Program (SEMP) which provides routinely scheduled preventative maintenance at overseas facilities.

8H. Waivers

1. Office Building Physical Security Standards

It is expected that all of the security standards contained in 8A1, will be met in newly constructed office buildings, and to the greatest extent feasible, in existing facilities. If, for any reason, a proposed facility cannot be modified to meet one or more of the standards, a waiver to the applicable standard(s) must be requested and approved prior to acquisition. This waiver procedure is designed to meet the accountability provisions of The Diplomatic Security Act. The following describes the process for seeking waivers to physical security standards:

a. USAID preparation of a packet of information containing:

(1) Basis of requirement for additional office space, e.g., Mission operational requirements, increase in staff level, or loss of lease on existing office space.

(2) Number of U.S. direct-hire personnel to be located within the space.

(3) Identification and description of proposed building/space. Description is to include building setback from vehicle access points, e.g., the street; whether there is underground parking in the building; basic construction of the facility, e.g., concrete slab with hollow block exterior walls; identification of bordering properties and surrounding area, e.g., building is located in a commercial district bordered on the south and west sides by commercial offices, on the east by a parking lot, and fronts on the street; photographs of the proposed facility; scale drawings of compound and/or building floor plans.

(4) Specific physical security standard(s) requested for waiver consideration. If the standard is other than the 100-foot setback requirement, the rationale for waiver of this standard must also be included, e.g., waiver of safehaven standard due to inadequate building floor load capacity.

(5) The availability of office space meeting security and USAID operational requirements within the city. Include the number of facilities reviewed in concluding that the proposed facility is the optimum choice.

(6) A security plan for the facility; specifically, what protection does the facility afford against vehicle ramming, terrorist attack, mob violence and what measures will be undertaken to minimize deviations from the security standard(s). Assistance and recommendations from a professional security officer will be required in developing the security plan.

(7) Estimated cost of implementing the security plan and whether the USAID has requisite funding available.

(8) Recommendations by the RSO concerning the application for waiver.

(9) Approval by the Chief of Mission.

b. The packet is forwarded to M/SER/MS for approval to lease/purchase the proposed facility.

c. If M/SER/MS concurs in the acquisition of the space, the packet is forwarded to the Office of Security. Office of Security reviews the security plan, prepares an endorsement and forwards it to the Bureau of Diplomatic Security (DS/PSP/PSD).

d. PSD reviews the packet, ensures RSO and Ambassador comments are included therein, and forwards the packet with appropriate comments and recommendations to the Assistant Secretary of Diplomatic Security who will convene the Security Standards Committee to review the request for final determination.

e. PSD notifies Office of Security of decision. Office of Security notifies M/SER/MS. M/SER/MS notifies the USAID whether acquisition of the space will be authorized.

2. Classified Storage Requirements

If the classified storage requirements contained in 8A3 cannot be met, a request for waiver will be required. The waiver to classified storage requirements is requested in writing through the RSO.

CHAPTER 9

SECURITY PROCEDURES

9A. Authorities

1. Department of State, Bureau of Diplomatic Security publication entitled: Establishment and Management of Local Guard Programs, published February, 1988.

2. Agency for International Development - Department of State Overseas Security Agreement, December 7, 1987

9B. Purpose

This chapter provides the requirement for establishing security procedures for the USAID security program.

9C. Definitions

1. U.S. Staff

U.S. direct-hire personnel and U.S. long term O&E funded Personnel Services Contractors.

2. USAID Staff: All employees of the USAID.

9D. Policy

1. Security procedures must be established and implemented at each USAID. The procedures shall ensure that the physical security systems and other security measures delineated in Part IV will be effective. The implementation of security procedures is the responsibility of the USAID.

2. Security procedures must insure, as a minimum, the following:

a. Access to the USAID facility is restricted to authorized personnel and vehicles.

b. Access to USAID office space is restricted to authorized personnel.

c. Effective visitor and package screening is conducted.

9D2

d. U.S. control of the USAID office space is constantly maintained.

9E. Security Procedures

1. Guards

Guards are to be employed both on the USAID compound and in the Public Access Control (PAC) area. In accordance with 9A1, the RSO is responsible for ensuring that there is a written set of guard orders covering both routine and emergency duties for each guard position. A copy of the guard orders will be provided to the USO by the RSO. Guard duties will include the requirements of 9D2a, b and c and locking of any exterior doors in the event of an emergency condition. The RSO may rely on the USO to assist in ensuring the guards perform their assigned duties.

2. Public Access Control

A security controller (typically the receptionist), will be employed to control entry into the building. It is recommended that this individual should be a U.S. citizen with local language capability. The security controller will occupy the area where the security door and alarm controls are located. As is the case for guards, the security controller is responsible for both routine and emergency security duties. The duties shall be written by the USO and remain at the controller's post. An example of the duties is provided in attachment 9A.

3. USAID Wardens

Depending on the size and configuration of the USAID office space, a warden system may be necessary. A warden system is typically recommended for multiple floor office buildings. Wardens can be utilized to provide assistance in the implementation of routine and emergency security plans. A warden system can be established to conduct routine checks of security doors to determine if the locks will engage, to establish individual responsibility for emergency locking of forced entry locks, or to assist in bomb searches, evacuation, or movement of personnel to the safehaven.

4. U.S. Staff

The U.S. staff duties include the security of classified and Limited Official Use material and maintaining U.S. control of the building. Specifically:

9E4

a. Access to classified material is limited to the U.S. staff. Classified material is maintained in authorized areas, stored in the authorized areas only, and transported (within, into, and out of the building) in accordance Confidential 1987 State Cable 324710 and 5 FAM 900. Classified material should be transmitted between the Embassy and USAID facility by a cleared U.S. direct-hire employee in a USAID official vehicle.

b. Access to the USAID building is under U.S. control at all times. When personnel are inside the USAID office space, a U.S. staff member will be present and will be responsible for the security of the facility; this is normally the senior USAID official present.

c. The USAID office will be locked by a U.S. staff member. Keys to the facility are to be kept to a minimum number and maintained at the Chancery or other location designated by the RSO. Any other duplicate keys may only be maintained by a limited number of U.S. staff members. The USO will be responsible for a key control program. The USO may consider a USAID duty officer system. Duties of the duty officer may include opening and closing the office, maintaining keys to the facility and/or picking up and dropping off the keys at the Chancery.

5. USAID Staff

The USAID staff is responsible for both routine and emergency duties. These duties shall be published in a standard operating procedure (SOP) accessible to the staff. The SOP will include visitor escort requirements and procedures for handling of National Security Information and Limited Official Use information. Emergency duties identified in the SOP will affix responsibilities for securing and or destroying classified and LOU material. It will also include the conditions for and the specific procedures of an evacuation, the fire plan, bomb threat plan, bomb search plan, and the alarm signal meanings.

ATTACHMENT 9A

SECURITY CONTROLLER DUTIES (SAMPLE)

The following is not all inclusive but provides basic security duties.

1. Routine Duties

a. Obtains identification and points of contact for all visitors; verifies points of contact with USAID U.S. staff to determine whether visitor may be allowed entry into USAID office space. The security controller notifies the PAC lobby guard that visitor entry will or will not be permitted. If entry is authorized, the visitor shall require an escort (USAID staff employee). Entry is not to be permitted until the escort arrives.

b. Conducts periodic checks and tests of the security systems. As a minimum, these will include a check of: the security door control (working status of switches and indicator lights); security door emergency locks; alarm system; any telephone and or other communications equipment at the security controller station (booth).

c. Maintains an awareness of activity in the lobby to ensure unauthorized persons do not gain entry into USAID office space, that the PAC lobby guard is not under duress (being threatened with a weapon), and that packages of unknown content have not been left in the lobby.

2. Emergency Duties

a. Telephonic bomb threat procedures

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: (1) notifies USO, senior USAID official, and or RSO/PSO (specific procedure as prescribed by USO); (2) activates bomb threat alarm as directed.

b. Terrorist or mob attack procedures

First, activates all security door emergency locks; Second, activates terrorist attack alarm; Third, notifies USO, senior USAID official, RSO/PSO and host government police/military forces (specific procedure as prescribed by USO and contained in instructions); Fourth, activates forced entry locks on those security doors under responsibility of security controller.

CHAPTER 10

OPERATIONS SECURITY

10A. Authority

National Security Decision Directive (NSDD) 298, "National Operations Security Program," January 22, 1988

10B. Purpose

This chapter establishes an AID Operations Security (OPSEC) awareness program.

10C. Objective

The objective of the AID Operations Security (OPSEC) awareness program is to ensure that reasonable security measures are employed to prevent the inadvertent compromise of classified or sensitive information. An effective OPSEC awareness program can contribute significantly to the overall security posture of AID Washington and USAIDs, particularly those situated in high threat environments. The term sensitive is that information which, if compromised, may adversely affect the safety or security of personnel and facilities.

10D. Vulnerabilities

1. While classified and LOU material is routinely destroyed by shredding or other approved methods, large volumes of unclassified material generated in Washington and overseas is normally discarded as trash. When the unclassified material leaves the custody of AID, no one can predict with any degree of certainty, the bona fides of who may be reading it.

2. Individual pieces of unclassified paper generated by AID may not appear to be significant; however, when examined in the aggregate, they may reveal sensitive data. The data may cause a hostile intelligence service or terrorist group to pay closer attention to AID activities. For example, unclassified copies of planning conference notes, proposed travel itineraries, new staffing patterns, and telephone directories which include employee position titles and home addresses, may be exploited.

3. The spoken word is also vulnerable to exploitation. In AID Washington and overseas, unclassified but sensitive information is often discussed in public places such as cafeterias or in other social gatherings. Modes of public transportation, including shuttle buses or commuter vehicles, are also used to discuss work. In the overseas environment, IG/SEC radios provided to employees provide a reliable means of communication. Using incorrect radio procedures such as associating call signs with specific employees, excessive transmission time, and discussing itineraries, can be exploited by anyone monitoring USAID radio frequencies.

10E. OPSEC Measures

Effective measures to protect sensitive information will eliminate indicators of its existence while concurrently projecting a routine, business-as-usual image. While the following measures may be considered basic security practices, incorporating them into a daily routine may also ensure future operational success. Recommended measures include:

1. Daily destruction of excess copies, drafts, and other materials used in the preparation of official correspondence.

2. Use of established radio procedures including call signs for personnel and location checkpoint designators; limiting transmission time and insuring that locations of key personnel and travel itineraries are not broadcast in the clear for unauthorized persons to intercept.

3. Instilling in employees a need to exercise caution in what they discuss at social gatherings or in other public places. The principle of "need-to-know" and confining work-related discussions to the work place must be observed.

4. Controlled dissemination of information concerning the travel of all AID personnel to and from post or within country. Travel itineraries should be marked as Limited Official Use and disseminated on a need-to-know basis when warranted by the threat situation. The travel itinerary of the AID Administrator or other designated AID officials shall be protected at the Confidential level.

10F. Responsibilities

1. The primary focal point in AID/Washington for operations security matters is IG/SEC.

10F

2. At post, the senior USAID official is responsible for insuring that all U.S. direct-hire and personal services contractors, commensurate with their positions and levels of security clearances, are made aware of and understand, at a minimum, the threats from hostile intelligence and the local intelligence/security service.

3. The senior USAID official will coordinate with the RSO and notify IG/SEC of any USAID activity which may impact adversely on operations security.

4. The senior USAID official is responsible for designating a U.S. direct-hire employee as the point of contact for OPSEC matters effecting the USAID.

5. The USAID OPSEC officer will assist the senior USAID official in implementing an OPSEC awareness program. In concert with the RSO, the officer will conduct appropriate threat briefings for USAID personnel. Appropriate records shall be maintained which identify the content of briefings, date(s) presented, and persons attending. Records will be maintained for two years. The USAID OPSEC officer will advise the senior USAID official of any practice which impacts adversely on operations security.

CHAPTER 11

SECURITY COMMUNICATIONS

11A. Authorities

1. The Inspector General Act of 1978, as amended, (P.L. 96-533 and P.L. 97-113)

2. The Foreign Assistance Act of 1961 as amended (22 USC 2349aa-4).

3. AID Administrator's memorandum dated May 5, 1987.

11B. Purpose

This chapter sets forth policy, fixes responsibilities, and establishes procedures for the IG/SEC Security Communications Program.

11C. Definitions

1. Base Station. A fixed radio which may include a separate power supply and is not normally intended for portable use.

2. Call Sign. Short alpha/numeric designator used to identify radio users or locations.

3. High Frequency Single Sideband. Type of communications system, in the high frequency range, for long distance communications.

4. Mobile Radio. A radio that is permanently installed in a vehicle and operates on the post Emergency and Evacuation (E&E) channel.

5. Network. (Net) Radio channel specified for use as a specific function (e.g., Emergency and Evacuation (E&E) channel, or administrative channel).

6. Project Radios. Radios procured either by the USAID or project contractor specified as integral to the project and to be turned over to the host government upon completion of the project. Project radios do not operate on the post Emergency and Evacuation (E&E) channel.

7. Residential Radio. A portable radio located in the bedroom or safehaven for emergency or administrative communications; it operates on the post Emergency and Evacuation (E&E) channel.

11C

8. Security Radios. Any radio operating on the post Emergency and Evacuation (E&E) channel.

9. T99 Selcal. Mode of radio operation similar to paging (beeper) systems found in the United States.

11D. Policy

1. General

a. The IG/SEC security communications program is designed to provide a two-way radio communications link from USAID office buildings and residential dwellings into the post Emergency and Evacuation (E & E) radio net.

b. USAID security radio communication systems shall include: the same E & E frequencies used by the Embassy, a residential security radio for every USAID U.S. direct-hire, PASA/RASA, and IDI employee, and a base station or residential type security radio at each USAID office building. Each heavy armored vehicle (HAV) and each light armored vehicle (LAV) shall have a mobile security radio. Other USAID official vehicles will be equipped with mobile security radios when necessary.

2. Funding and Acquisition

a. Funding support for USAID security radio communication systems is provided by IG/SEC. Any separate administrative radio requirements shall be funded by USAIDs.

b. IG/SEC does not provide funding for radios for loan to other Agencies. Foreign Service Nationals (FSN) radio requirements will be determined by IG/SEC on a case-by-case basis. Factors used to make this determination will include: post threat assessment, FSN duties, security responsibilities, and USAID recommendation.

c. USAIDs will determine their security radio system requirements annually, during the second quarter of the Fiscal Year. The requirement for any additional radio system components will be made to IG/SEC via cable. The cable should include a brief justification to include the user's name and job title. An unused T99 selcal number should be obtained from the Embassy Communications Program Officer (CPO) for each radio requested, whether or not T99 is in use at Post.

d. USAIDs will issue the purchase orders for their security radio system requirements directly to vendors, utilizing the funding citation provided by IG/SEC for procurement. IG/SEC shall also provide USAIDs with all necessary technical and vendor information to enable them to initiate purchase orders. Each purchase order shall:

(1) List IG/SEC as delivery point.

(2) Specify that the purchase order number must be placed on the shipping label.

(3) Specify that the invoice accompanying the equipment and the purchase order itself includes the following information: the purchase order number; the number and specific type of equipment ordered; the identity of the organization issuing the purchase order; the ultimate destination (city and country) of the equipment; each frequency required; the selcal number for each radio, and the serial number.

e. USAIDs will forward copies of purchase orders to AID/Washington, Attention: IG/SEC/PS/SC, Washington, D.C. 20523-1604.

f. Upon receipt of the equipment from the vendor, IG/SEC will perform Federal Communications Commission (FCC) performance tests to insure proper operation. Upon completion of testing, the equipment will be forwarded to USAIDs. USAIDs will be notified of shipment information.

g. All orders for USAID administrative radio requirements and all orders for contractor security radio requirements must be referred to IG/SEC for review prior to procurement.

3. Accountability

USAIDs are accountable for all security radio equipment. Radio equipment is considered non-expendable property, except for certain auxiliary items, e.g., antennas, coax cables, and non-repairable batteries. All security radio equipment (less project radios) will be entered into USAID accounts regardless of funding source or whether used by direct-hire employees or contractors. In case of staff reduction or USAID closure, all security radio equipment must be transferred to IG/SEC. Inventory discrepancies must be reported to IG/SEC.

4. Radio Repair

a. AID security radios can be repaired by one of the following methods: (1) At USAID expense, by an authorized factory representative in country, (2) at USAID expense, except for parts, by an FSN or TCN hired by the USAID and certified by IG/SEC, (3) at USAID expense by a USAID-hired contractor and certified by IG/SEC, (4) at IG/SEC's expense, by pouching the radio to IG/SEC, if the other measures are not possible.

b. Radios sent to IG/SEC must be accompanied by a written description of the problem, radio model number, serial number and T99 selcal number. Cables providing pertinent information should be sent to IG/SEC/PS/SC as soon as possible.

5. Radio Batteries and Charging Units

a. All new radios shipped to USAIDs will be supplied with a new battery and charging unit by IG/SEC. USAIDs are responsible for replacing batteries and charging units.

b. Upon request, IG/SEC will provide battery and charging unit pricing and vendor information to USAIDs for purchase order preparation.

6. Contractor Radios

a. All contractor radio requirements shall be funded by USAIDs or through applicable contracts (both project and security radios). IG/SEC will test and ship security radios for contractors. USAIDs must contact IG/SEC for advice on approved equipment and pricing. Purchase orders issued for contractor security radios shall include the same information required in paragraph 11D2d above.

b. Maintenance and repair of contractor security radios is the responsibility of USAIDs. If there are no locally available repair facilities, USAIDs should contact IG/SEC/PS/SC for information on shipment of radios to alternate facilities, e.g., authorized vendor representatives elsewhere in the region or in the U.S.

c. Security radios purchased for project contractors will be returned to IG/SEC for disposition when the project is completed.

11D

7. HF SSB and Project Radio Systems

a. HF SSB systems are used at USAIDs to provide long-haul communications. USAIDs interested in establishing HF SSB systems should contact IG/SEC for equipment costs, vendor addresses, host country licensing procedures, and other information.

b. IG/SEC can assist USAID projects with two-way FM radio requirements. Assistance will range from recommending actual equipment or systems to facilitating USAID contact with appropriate vendors. IG/SEC does not fund, install, or maintain project two-way FM systems.

11E. Responsibilities

1. IG/SEC

IG/SEC exercises oversight of USAID security communications systems. IG/SEC communications specialists perform system inspections, system modifications, equipment installations, and repair functions.

2. USAID

USAIDs are responsible for all AID-owned or purchased security radio equipment. This responsibility includes routine maintenance, care, operation, and accountability.

3. USO

The USO serves as the USAID security communications program manager. The USO will ensure that radio users are knowledgable on use of the radios. USAID requests for post visits by IG/SEC communications specialists should be requested by cable, identify the scope of work, and be as far in advance as possible.

4. Radio User

a. All USAID radio users are responsible for insuring that individual radios are operational and maintained.

b. Embassies normally conduct two-way radio checks on a monthly basis. USAID radio users must participate in these checks. If a user is unable to participate in a scheduled check, the user should request a radio check.

c. All family members should know how to operate the radio assigned to the family.

CHAPTER 12

ARMORED VEHICLES

12A. Purpose

This chapter establishes an AID armored vehicle program.

12B. Definitions

1. Armored Vehicle

An armored vehicle is an official vehicle that has been modified to carry specific types of opaque and transparent armor. The armor systems are designed to defeat multiple impacts of ballistic rounds. The armor is designed for placement in the vehicle without noticeably changing its outward appearance. Armored vehicles are either lightly or heavily armored.

2. Light Armored Vehicle (LAV)

LAVs s are treated with special types of opaque and transparent materials which afford the occupants protection against some small arms.

3. Heavy Armored Vehicles (HAV)

HAVs are treated with opaque and transparent materials which afford the occupants protection above the LAV.

12C. Objective

The objective of the IG/SEC armored vehicle program is to provide vehicles that have been specially armored to protect the occupants against ballistic attack from a variety of small arms. Terrorist tactics frequently take the form of kidnapping or assassination. Experience has shown that travel between home and office, or other destination, is the period when employees are most vulnerable to these threats. The combination of the vehicle's armor and its mobility are intended to provide protection and enable personnel to leave the area of threat.

12D. Policy

1. Light armored vehicles are authorized at USAIDs situated in certain high threat posts. Normally, only passenger-carrying vehicles used by the senior USAID official or other designated employees are lightly armored. At those locations where a home to office and return shuttle service has been established by the post, all shuttle vehicles will be lightly armored.

2. Heavy armored vehicles are normally assigned to USAIDs at very high threat posts. Because of the high costs of these vehicles, IG/SEC normally will not provide the vehicles unless there are demonstrated threats against the U.S. community and the RSO endorses the requirement.

3. Light or heavy armored vehicles must be used only for official purposes. Heavy armored vehicles shall not be left unattended when they are outside a U.S. controlled motorpool. The loss and subsequent damage to or destruction of a heavy armored vehicle caused by negligence, shall be considered grounds for disciplinary action.

12E. Maintenance and Funding

1. Maintenance

USAIDs are responsible for the maintenance of light and heavy armored vehicles.

2. Funding

IG/SEC is responsible for procurement of the HAV. The LAV is a vehicle purchased by the USAID. Funding responsibility of IG/SEC for the LAV is limited to the cost of application of the armor.

12F. Reassignment of Heavy Armored Vehicles

IG/SEC retains the right to transfer vehicles from post based upon operational and security requirements.

12G. Budgeting for LAVs

USAIDs will inform IG/SEC of their projected two year LAV requirements during the annual budget formulation process which occurs in April. USAIDs should cable their requirements to IG/SEC/PS with sufficient lead time to ensure they are incorporated into the IG budget. Unprogrammed LAV requirements will be funded by IG/SEC only when warranted by exceptional circumstances which are beyond USAID control.

CHAPTER 13

OVERSEAS RESIDENTIAL SECURITY

13A. Authorities

1. Department of State, Bureau of Diplomatic Security publication entitled: Residential Security Program Guidance, published March, 1987.

2. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399) (Diplomatic Security Act)

13B. Purpose

This chapter describes the overseas residential security program and delineates responsibilities for program management.

13C. Program Administration

The residential security program is administered and funded by the Department of State. Post implementation of this program is under the purview of the RSO with funding support provided by DS/PSP/RSG.

13D. Department of State Policy

1. It is the policy of the U.S. Government to take all reasonable and appropriate steps to reduce the risks of employees and their dependents to terrorism and high levels of criminal activity while they are serving abroad. If the host government is incapable or unwilling to take the appropriate steps to protect assigned American personnel and their dependents, as they are required to do under international law, then serious consideration will be given to withdrawing endangered personnel. Security steps taken by the U.S. Government are therefore, designed to complement and enhance the efforts of the local authorities. To this end, financial and human resources will be committed in an attempt to ensure a safer environment for our employees and their families.

2. The intent of this program is to provide an equal level of protection to all U.S. citizen direct hire employees at each diplomatic mission. The components of the residential security program include application of locks, alarms, exterior lighting, grillwork, and safehaven areas to the residences of direct hire U.S. employees. The complete program is contained in 13A1.

13E. AID Policy

1. All USAID requests for residential security upgrades and/or funding are to be forwarded directly to the RSO with an information copy to IG/SEC. Responsibility for notifying the RSO of USAID residential security requirements rests with the USAID.

2. Department of State funding for the residential security program applies only to U.S. direct-hire employees. All residential security equipment requirements for contractors (long term Personnel Services Contractors (PSC) or project contractors) shall be funded through the applicable contract. USAIDs should establish a parallel residential security program for U.S. contractors. USAIDs should coordinate with the RSO to determine costs for the purchase and installation of requisite equipment for contractor personnel and program funds accordingly.

3. In cases of emergency or extraordinary circumstances, the senior AID officer is authorized to enhance residential security for USAID U.S. employees and contractors from existing budgets. Enhancements of this nature must be coordinated with the RSO, post Emergency Action Committee, and IG/SEC.

CHAPTER 14

OVERSEAS LOCAL GUARD PROGRAM

14A. Authorities

1. Department of State, Bureau of Diplomatic Security publication entitled: Establishment and Management of Local Guard Programs, published February, 1988.

2. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399) (Diplomatic Security Act)

14B. Purpose

This chapter describes the overseas local guard program and delineate responsibilities for the program management.

14C. Program Administration

The local guard program is administered and funded by the Department of State. Post management and implementation of this program is the responsibility of the RSO.

14D. Department of State Policy

The Department of State is responsible for providing a secure environment in which to conduct the business of the U.S. Government at Foreign Service posts. This responsibility embraces all agencies of the U.S. Government which are normally associated or co-located with diplomatic and consular establishments and under the control of the Chief of Mission. Part of this environment is provided through the development of a Local Guard Program (LGP) which includes the use of local guard force personnel for access control, building and residence security, and sometimes for personal protection of key personnel. LGPs are primarily intended to provide services that the host government is unable or unwilling to provide despite a formal request to do so (Chapter 1 of 14A1).

14E. AID Policy

1. USAID local guard requirements shall be forwarded to the RSO for inclusion in the post local guard program. Funding for Embassy requirements is provided by DS/PSP/RSG. The policy for funding USAID local guard programs is established in AID Washington.

14E

2. The local guard program applies only to official U.S. facilities. All local guard requirements for contractors and contractor facilities shall be funded through the applicable contract. USAIDs should coordinate with the RSO to determine contractor guard costs and program funds accordingly.

CHAPTER 15

CONSTRUCTION AND TRANSIT SECURITY

This chapter is reserved for the security requirements pertaining to construction of new office buildings and the security requirements for the transit of materials destined for core areas within a new building.

CHAPTER 16

RESERVED

TAB V - SECURITY AWARENESS AND TRAINING PROGRAM

TAB 5

SECURITY AWARENESS AND TRAINING REQUIREMENTS

This part describes the security awareness and training requirements. The goal of this program is to ensure all personnel are knowledgable of requirements, systems, and procedures that are intended to prevent terrorists, criminals, and other hostile groups from causing injuring to AID personnel and to preclude the compromise of national security information.

TABLE OF CONTENTS

Chapter 17 - Counterintelligence Awareness
Chapter 18 - Security Awareness and Training Program
Chapter 19 - Security Personnel Training (Guards, Drivers, USOs, Receptionists, Employees)
Chapter 20 - (Reserved)
Chapter 21 - (Reserved)

CHAPTER 17

COUNTERINTELLIGENCE AWARENESS

17A. Authorities

1. National Security Decision Directive 197, "Reporting Hostile Contacts and Security Awareness," November 1, 1985.

2. Executive Order 12333, "United States Intelligence Activities," December 4, 1981.

3. Director of Central Intelligence Directive 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)," July 20, 1987.

4. 11 FAM 236.3, "Conversations and Contacts with Communist Country Officials and other Nationals," September 26, 1980.

5. 79 State A-1299 "Guidance Regarding Relationships with Nationals of the Soviet Union and Certain Other Communist Countries," April 20, 1979.

6. 76 State A-3010 "Personnel Travel to the Soviet Union and Eastern Europe by All U.S. Government Personnel and Their Adult Dependents Attached to American Diplomatic and Consular Posts," June 16, 1976.

7. Limited Official Use (1982) State Cable 209456, "Clearance Procedures for U.S. Government Employees and Adult Dependents Visiting the Soviet Union, Eastern Europe (Except Yugoslavia) the PRC and Cuba."

8. Foreign Affairs Manual, Volume 12, "Diplomatic Security."

17B. Purpose

1. This chapter implements the provisions of NSDD 197 within AID. It establishes policy, assigns responsibilities, and prescribes procedures for reporting contacts with citizens of Communist, Communist-controlled, or other countries/entities whose policies are inimical to the interests of the United States.

2. This chapter also establishes requirements for the periodic briefing of AID employees on hostile intelligence and outlines personnel reporting requirements. It prescribes disciplinary or administrative sanctions for AID personnel who fail to comply with the requirements stated herein.

17C. Definitions

1. National Security Information

Official information that relates to our national defense or foreign relations. National security information may be classified as Top Secret, Secret, or Confidential.

2. Counterintelligence

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.

3. Espionage

The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense foreign policy with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies in time of war or peace.

4. Sabotage

An act or acts with the intent to injure, interfere with, or obstruct the national defense or foreign policy of a country by willfully injuring, destroying, or attempting to destroy national defense or war material, premises, or utilities, to include human or natural resources.

5. Terrorism

The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.

6. Contact

Any form of meeting, association, or communication; in person, by radio, telephone, letter or other means, regardless of who initiated the contact or whether it was for social, official, private, or other reasons with a citizen or entity of a Communist, Communist-controlled or criteria country. A contact has occurred even if no official information was discussed or requested.

17C

7. Criteria Country

Criteria countries are listed in 11 FAM 236.6. and 12 FAM.

8. Entity

An embassy; consulate; trade, press, airline, cultural, tourist, or business office; and any organization representing a Communist, Communist-controlled, or criteria country.

9. AID Employee

For the purpose of this program, AID employees include full-time and part-time U.S. direct-hires and U.S. contractors.

17D. Policy

1. All AID employees and contractors are required to report information or circumstances that could pose a threat to the security of AID employees, facilities, or national security information. In AID/Washington, reports shall be provided to IG/SEC. Employees serving overseas shall provide reports of contact to their respective Regional Security Officers.

2. All AID employees will receive periodic briefings on hostile intelligence and terrorist threats. The briefings are sponsored by the Office of Security and are conducted in Washington and at USAIDs overseas. Attendance at these briefings is mandatory for all employees.

3. All AID employees traveling to criteria countries will request foreign travel briefings and be debriefed upon their return.

17E. Responsibilities

1. Assistant Inspector General for Security (AIG/SEC)

a. The AIG/SEC is responsible for developing, implementing and managing the AID counterintelligence awareness program.

b. The AIG/SEC is responsible for administering an appropriate briefing program to foster employee awareness of hostile intelligence and terrorist threats.

c. Investigations or inquiries to determine the circumstances surrounding reported contacts, harassment and provocation involving AID employees are the responsibility of the AIG/SEC. The Regional Security Officer will conduct investigations or inquiries overseas, on behalf of Office of Security, in accordance with the terms of the AID - Department of State Overseas Security Agreement. The Office of Security will initiate appropriate investigations or inquiries involving AID/W personnel.

d. The AIG/SEC is also responsible for conducting liaison with federal law enforcement, intelligence and security agencies on matters affecting the AID security posture.

2. USAID Director

a. The USAID Director or senior AID official is responsible for implementing an effective counterintelligence awareness program within the USAID in concert with the Regional Security Officer.

b. In implementing the program, the USAID Director or senior AID official must insure that all USAID employees receive appropriate training.

c. The USAID Director or senior USAID official is responsible for insuring compliance with the reporting requirements contained in IG.

3. Principal Security Officers in AID/W

a. Principal Security Officers in AID/W are responsible for notifying the Office of Security in instances where employees of their organization report contacts.

b. Principal Security Officers are also responsible for insuring that employees are included in scheduled counterintelligence awareness briefings.

4. AID Employees

a. AID/Washington employees are responsible for reporting actual or suspected contacts when they have reasonable cause to believe that they have been approached. Contacts must be reported to the Office of Security.

b. AID employees serving overseas are required to report actual or suspected contacts to the Regional Security Officer.

17E4

c. AID employees are also responsible for attending scheduled counterintelligence awareness training.

17F. Guidance

1. The references cited in 17A form the basis for implementing the AID counterintelligence awareness program.

2. USAIDs shall maintain written records which show employee attendance at counterintelligence awareness training. At a minimum, the records shall contain the name of the employee, date(s) of training, topic(s), location of training, and name of the instructor. The records should be retained for a minimum of two years after completion of the training. The training records shall be made available to Office of Security inspectors during inspection visits.

17G. Reporting Requirements

1. All contact reports will be in written form, marked Confidential, and protected from general distribution. Reports shall be completed in accordance with the provisions of 12 FAM. Personnel overseas should contact the RSO for assistance. In AID/W, IG/SEC will provide appropriate guidance.

2. Contact reports will be distributed on a "need-to-know basis" as follows:

a. For AID/Washington

(1) Employees shall provide their written contact reports to IG/SEC.

(2) Employees will not discuss their reporting of actual or suspected contacts with representatives of criteria countries to persons outside the security arena.

b. For USAIDs

(1) Employees will advise the Regional Security Officer when they have reason to believe that they have been contacted by hostile intelligence services or other entities as defined in 17C8.

(2) In the event that a Regional Security Officer is not resident at the post, the USAID Director or senior AID official should be advised of the details of the contact. The USAID shall subsequently notify the post security officer.

17H. Compliance

1. Office of Security inspection visits to USAIDs will include an evaluation of the program's effectiveness and USAID compliance.

2. Should an employee intentionally fail to report an actual or suspected contact as called for in 1G, the AIG/SEC may forward a recommendation for appropriate disciplinary or administrative action to the Director, Office of Personnel Management (PFM/PM).

CHAPTER 18

SECURITY AWARENESS AND EDUCATION

18A. Authorities

1. The Inspector General Act of 1978, as amended, (P.L. 95-452 and P.L. 97-113)

2. Executive Order 12356, "National Security Information," April 6, 1982

3. ISOO Directive 1, "Information Security Oversight Office", June 25, 1982

4. Uniform Security Regulations (5 FAM 900), September 1985

5. Agency for International Development - Department of State Overseas Security Agreement, December 7, 1987

18B. Purpose

This chapter describes AID's Security Awareness and Education Program, establishes policies and procedures for the program, and assigns responsibilities for its implementation. The program is designed to strengthen security by increasing the knowledge and motivation of individuals having responsibility for the protection of personnel, facilities and national security information.

18C. Applicability

The Security Awareness and Education Program described in this chapter applies to all AID direct hire employees, contractors, and associates.

18D. Policy

1. All AID employees and cleared contractors will attend initial security training prior to being given access to national security information. Attendees at the training will be required to execute the SF 312 "Classified Information Non-Disclosure Agreement." If briefed overseas, the SF 312 shall be forwarded to IG/SEC for retention within the employees' security file.

18D

2. All AID employees will receive security briefings on a bi-annual basis. Attendance is mandatory for all employees assigned to non-critical sensitive, critical sensitive or special sensitive positions. This requirement is amplified in Tab 2 (Information Security Program).

3. All AID employees will receive a security debriefing prior to separation. The debriefing will be administered by the local designated security official. Attendance at the debriefing and execution of the "Security Debriefing Acknowledgement" portion of the SF 312 is mandatory. The completed SF 312 will be forwarded to IG/SEC for retention when separation occurs outside AID/W.

4. All executive/management officer designates will attend the Unit Security Officer Course presented in AID/W prior to their assignment to post.

5. All AID employees destined for an overseas assignment will attend the Department of State's Seminar On "Coping With Violence Abroad" prior to assignment overseas.

6. Personnel cleared for access to LOU only will be required to sign AID Form 6-97 prior to being granted access, and AID form 6-98 upon their separation.

18E. Responsibilities

1. Assistant Inspector General for Security (AIG/SEC)

a. The AIG/SEC has responsibility for developing, implementing and managing the Agency's Security Awareness and Education Program.

b. The AIG/SEC has responsibility for administering an appropriate briefing program to foster employee awareness of hostile intelligence and terrorist threats.

2. USAID Director

a. The USAID Director or senior AID official is responsible for implementing an effective security awareness program within the USAID in concert with the Regional Security Officer.

b. In implementing the program, the USAID Director or senior AID official must insure that all USAID employees receive appropriate training.

c. The USAID Director or senior USAID official is responsible for insuring compliance with the reporting requirements contained in 2I.

3. Principal Security Officers (PSO) in AID/W

a. PSOs in AID/W are responsible for ensuring that employees are included in scheduled security awareness briefings.

b. PSOs are also responsible for notifying IG/SEC when employees of their organization receive security awareness training.

4. Unit Security Officers (USO) Overseas

a. USOs overseas are responsible for attending scheduled Post Security Officer Training.

b. USOs are responsible for coordinating with the Regional or Post Security Officer to provide procedural training to mission personnel.

c. USOs are responsible for notifying IG/SEC in instances where employees of their organization receive security awareness training from the Department of State.

5. AID Employees

AID employees are responsible for attending scheduled security awareness training.

18F. Department of State Sponsored Training

1. Security Overseas Seminar

The Security Overseas Seminar addresses measures the U.S. government is taking to combat terrorism, and safety techniques that may be useful for individuals living in a potentially hostile overseas environment. The seminars are sponsored by the Foreign Service Institute and are conducted in Washington. Attendance is mandatory and may be scheduled through the AID Training Division.

2. Diplomatic Security Antiterrorism Course

This four-day course is conducted at a training facility south of Waldorf, Maryland and supplements the Coping With Violence Abroad Seminar. The course covers surveillance detection, search and

recognition of explosive devices, safe use of revolver and shotgun, evasive driving maneuvers and practical skills to enhance individual personal security. Attendance is voluntary and may be scheduled through the AID Training Division.

3. Mobile Training

Mobile Training courses are presented on an ad hoc basis and cover a variety of security topics. The courses are sponsored by the Diplomatic Security Bureau and are presented at overseas locations. Attendance for AID employees is voluntary and may be scheduled by the USO in coordination with the Regional or Post Security Officer.

4. Post Security Officer Training

This five-day course is sponsored by the Diplomatic Security Bureau in Washington and overseas. The course covers facilities, information, personnel and procedural security. USOs are strongly encouraged to attend. The course is voluntary for executive/management officer personnel and may be scheduled in coordination with the Regional or Post Security Officer.

5. Film and Video Distribution

The Diplomatic Security Bureau maintains a library of films and videos on a variety of security topics. The films and videos are available in several formats for loan to USAIDs worldwide. A listing of materials may be obtained from the Department of State. Viewing of security films and videos is voluntary for AID employees and may requested through the USO in coordination with the Regional or Post Security Officer.

18G. AID Sponsored Training

1. Initial Information Security Brief

This briefing is sponsored by the AID Training Division and is presented in Washington by an IG/SEC security professional. The briefing covers individual responsibilities for protecting National Security Information. Attendance at the briefing is a prerequisite to being authorized access to classified material.

18G

2. Bi-Annual Security Refresher Training

The training is sponsored by IG/SEC and is conducted in Washington and at USAIDs overseas. The purpose of the course is to revitalize individual awareness of the threat and reinforce proper protective procedures. Course material is topical and covers such subjects as hostile intelligence and terrorist threats.

3. Termination Debriefings

Termination Debriefings are presented by IG/SEC or Department of State security professionals prior to termination of employment. The purpose of the briefing is to determine whether the employee has had any known or suspected contact with criteria country foreign nationals and to reiterate the individual responsibilities to protect classified information even though the employee has been terminated. The briefings may be scheduled through the USO overseas in coordination with the Regional or Post Security Officer, or IG/SEC in AID/W.

4. Unit Security Officer Course

The Unit Security Officer Course is sponsored by the IG/SEC as part of the International Development Intern (IDI) Training Program. It is a comprehensive course covering facilities, information and personnel security. Course topics include security concepts and standards, measures to safeguard National Security Information, secure communications and security operations and procedures. The training is open to all executive/management officers and may be scheduled through M/SER/MS and IG/SEC.

5. Film and Video Distribution

IG/SEC maintains a library of films and videos on a variety of security subjects. The films and videos are available in several formats for loan to all USAIDs. A listing of materials may be obtained from IG/SEC. Viewing of security films and videos is voluntary for AID employees.

18H. Training Records

1. USAIDs will maintain written records which show employee attendance at security awareness training. The records shall contain the name of the employee, date(s) of training, topic(s), location of training, and name of the instructor. The records should be retained for a minimum of two years after completion of the training. The training records shall be made available to IG/SEC representatives during inspection visits.

CHAPTER 19

SECURITY PROCEDURES TRAINING

19A. Authorities

1. Department of State, Bureau of Diplomatic Security publication entitled: Establishment and Management of Local Guard Programs, published February, 1988.

2. Agency for International Development - Department of State Overseas Security Agreement, December 7, 1987

19B. Purpose

This chapter outlines the training requirements for USAID personnel assigned security duties.

19C. Objective

Training is critical to ensuring that security procedures are understood and implemented. Unless personnel react appropriately during a crisis situation, physical security systems may lose their effectiveness.

19D. Applicability

The training requirements in this chapter pertain to security personnel as defined below.

19E. Security Personnel

Security personnel are defined as those USAID employees whose duties include security responsibilities. Such personnel include the USAID Unit Security Officer, the guard force, the public access controller (receptionist), and other personnel whose duties may affect the USAID security program.

19F. Responsibilities

1. USAID Director

a. The USAID Director is responsible for ensuring that the USAID Unit Security Officer (USO) has received adequate training from the Regional Security Officer (RSO).

19F1

b. The USAID Director is responsible for ensuring that the USAID security personnel receive adequate procedural security training from the RSO.

2. USAID USO

The USO assists the RSO, as requested, and ensures that:

a. The security controller is trained and can respond to both routine and emergency situations.

b. The guards have received the necessary training from the RSO.

c. The RSO has provided security training to the drivers of HAVs and LAVs.

d. USAID wardens, U.S. staff, and USAID staff personnel are trained in routine and emergency duties (refer to Chapter 9, Security Procedures, concerning content of duties).

19G. Policy

1. All personnel must be trained and be ready to respond appropriately during a threatening situation.

2. Guards and the security controller must know how to properly carry out their emergency lock-up functions.

19H. Compliance

IG/SEC Security Inspections will include a determination of USAID compliance with the requirements in this chapter.

CHAPTER 20

RESERVED

CHAPTER 21

RESERVED

TAB VI - INSPECTIONS
AND REPORTING PROGRAM

TAB 6

INSPECTIONS AND REPORTING PROGRAM

This part describes the inspection and reporting program within the Agency. The goal of this program is to keep senior AID officers appraised of the security status of the Agency.

TABLE OF CONTENTS

Chapter 22 - USAID Security Inspections
Chapter 23 - USAID Incident Reports

CHAPTER 22

USAID SECURITY INSPECTIONS

22A. Authorities:

1. The Inspector General Act of 1978 as amended (P.L. 96-533 and P.L. 97-113)

2. The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399) (Diplomatic Security Act)

3. Agency for International Development - Department of State Overseas Security Agreement, December 7, 1987

22B. Purpose

1. This chapter delineates policy, assigns responsibilities, and establishes procedures for the conduct of inspections of USAID activities overseas by Office of Security.

2. The goals of the inspection program are to ensure USAID compliance with security requirements and standards for the protection of personnel, facilities, and national security information. The goal is also to ensure that the USAID is provided with the required security support by the Regional Security Officer.

22C. Applicability

The AID Office of Security Overseas Inspection program is applicable to all AID activities overseas.

22D. Scope

The scope of inspections will be based on the requirements contained herein or referred to in this handbook. Subject areas include security of USAID personnel, facilities, national security information, and security communications. The IG/SEC inspection report format is contained in attachment 22A.

22E. Policy

In accordance with the authority cited in 22A1, USAIDs will make available all records, reports, documents, recommendations or other material to representatives of Office of Security regarding those matters for which the Assistant Inspector General for Security (AIG/SEC) has responsibility.

22F. Reports of Inspection

A copy of the Inspection Report will be forwarded to the USAID and other offices as appropriate. USAIDs must provide a written response to IG/SEC within 45 days of receipt of the report. The response will indicate the status of all recommendations identified for USAID action. A format for the initial response is provided in Attachment 22B.

ATTACHMENT 22A

Office of Security

Inspection Report

USAID/_____

(DATE (MONTH & YEAR))

(signatures)

_____

IG/SEC Inspecting Officer: (name of Regional Operations Officer)

_____

IG/SEC/PS: (Division Chief)

_____

CONTENTS

PART I: EXECUTIVE SUMMARY

A. Introduction
B. Personnel Consulted
C. Summary of Findings
D. Summary of Recommendations
E. Action Summary

PART II: INSPECTION OF USAID SECURITY PROGRAM - AGENDA ITEMS

A. General
B. USAID Office Building Security
C. Information Security
D. Armored Vehicles
E. Residential Security
F. Personnel Security
G. Security Training and Awareness
H. Incident Reporting

PART III: EXHIBITS

A. Maps
B. Compound and Building Site Plans
C. Floor Plans
D. Photographs
E. Security Equipment Inventory
F. Other (as needed)

PART I

EXECUTIVE SUMMARY

INTRODUCTION

- o - Includes names of the person or persons on the inspection team.
- o - Date(s) of inspection
- o - Name/city of post visited

PERSONNEL CONSULTED

- o - Contains names and titles of key personnel consulted during visit

SUMMARY OF FINDINGS

- o - Contains brief summary of background leading up to the visit
- o - Contains brief summary of the visit, to include major findings
- o - Contains any comments that need to brought to the forefront of the report

SUMMARY OF RECOMMENDATIONS

- o - Contains a brief summary of the basic recommendations in numerical sequence; full details of recommendations are contained in the body of the report

ACTION SUMMARY

- o - Contains a summary of items for action by Post
- o - Contains a summary of items for action by IG/SEC
- o - Contains a summary of items for action by others as necessary

PART II

INSPECTION ITEMS

A. GENERAL

1. Identification of USAID: (Indicates if it is a Mission, USAID Representative, USAID Affairs Office, Regional Inspector General office, Regional Development Office, or other regional organization)

2. USAID Key Personnel: (Name of Mission Director, USAID Representative, USAID Affairs Officer, or Regional Director; also includes names and titles of other key personnel, e.g., Deputy Director, Executive Officer, USAID GSO)

3. Unit Security Officer: (Name of USAID USO and whether written designation has been made)

4. USAID, RSO and EAC Participation: (Indicates level of coordination with the RSO and frequency of USAID participation and attending officer(s); also indicates if USAID is included in Post Emergency Action Plan)

5. USAID Staffing Level: (Includes number of USDH, FSN DH, US PSC, FSN PSC, and TCN; also indicates whether there is any projected increase or decrease in USAID staffing)

6. Address - (Of location(s) being inspected)

7. Other USAID Facilities in Country: (Indicates if there is more than one AID organization, e.g., a Mission and a Regional Office; also indicates if there are other USAID offices located elsewhere in the country; includes address(s) of other USAID facilities and usage of these other locations, i.e. warehouses, offices, project offices, etc.)

8. Ownership/Lease Status- (Indicates if property is owned by USG or private parties; provide lease expiration date and terms for length of renewal)

9. Other Occupants - (Indicates business affiliation of occupants in buildings being shared with AID; nationality of company and personnel of shared buildings; whether building is shared with other U.S. personnel and what branch of U.S. government is involved)

10. Description of Surrounding Area - (Residential, business, governmental, etc; also includes locations of other diplomatic missions major reference points or other items of interest)

11. USO Reference Documents: (Indicates if USO has a copy of AID Handbook 6, USO Manual Book 1, USO Manual Book 2, DS Local Guard Program Manual, and DS Residential Security Guidance Handbook)

12. Regional Security Officer: (Indicates name and post of assignment)

B. USAID OFFICE BUILDING SECURITY

1. Description of Building: (Indicates type of construction materials used for walls, floors, and roof; height of building, other details as may relate to recommendations)

2. Physical Security Systems: (Indicates and describes physical security systems in place and compliance with the basic security standards)

a. Setback: (Describes distance from USAID building to outer perimeter, i.e., fence or wall)

b. Vehicle Control Barriers: (Describes bollards, planters, walls, and other traffic control devices employed)

c. Protective Window Film: (Indicates whether glass surfaces are treated with required type of protective film)

d. Perimeter walls/fences: (Describes walls, fences and/or pedestrian gates employed at the perimeter)

e. Public Access Control (PAC): (Describes the PAC system and whether it provides required level of ballistic and forced entry protection)

f. Building Exterior: (Describes the exterior walls of the building and any doors and windows in the building's exterior and whether the required level of ballistic and forced entry protection is provided)

g. Metal Detection: (Indicates whether metal detection devices, i.e., hand-held or walk-through metal detectors, are employed)

h. Emergency Notification: (Indicates whether there is an emergency notification system installed (alarm or PA system))

i. Safehaven: (Indicates whether there is a safehaven/safe area in the building and whether it contains: communications equipment, a means of egress, an ability to destroy classified holdings (connected to a reliable emergency power source), and emergency provisions such as rations, water, blankets, and first-aid kits)

j. Communications Equipment: (Describes equipment available in the building (and in safehaven) for communication with the embassy, local law enforcement offices, local government military forces, and guard force; equipment may include intercom systems, telephones, radios and antenna lead-in connection)

k. Exterior Lighting: (Describes type and quality of exterior lighting to include number of fixtures, type of switching, protection of wiring, and accessibility)

l. Ancillary Equipment: (Describes security equipment present at facility such as door control units, power supplies, CCTV, shredder, emergency lights, type and use of intrusion alarms or other alarm devices used for the AID facilities)

m. Emergency Power: (Describes emergency power source, e.g., a generator, including such information as make/model, KVA output, security equipment tied into the generator, location and protection afforded the generator, fuel supply location and capacity, responsibility for maintenance/service of the generator, and frequency of generator testing or percentage of actual operation)

3. Office Security Procedures:

a. Access Control: (Includes a description of access to the USAID facility and office space; indicates whether access is restricted to authorized personnel and vehicles; indicates if effective visitor and package screening is conducted; indicates if a security controller/receptionist is employed to control entry into the building and whether the duties are written and remain at the controller's post; also indicates whether the security controller/receptionist has received adequate security procedure training from the RSO, specifically, does the security controller know and carry out his/her emergency lock-up functions)

b. Guards:

(1) Local Guard Program: (Describes post local guard program: Indicates if USAID local guard requirements have been forwarded to the RSO for inclusion in the post local guard program; describes guard contract (one contract for the post, USAID separate guard contract, PSC guard contracts, etc.); identifies official responsible for USAID portion of guard force (RSO or USO); indicates total number of guards assigned to USAID facility (also refer to Part II E, Residential Security, which includes number of guards at USAID residences); includes nationality of guard supervisor and/or company; includes an overall assessment of the guards (good, adequate, poor))

(2) USAID Facility Guards: (Indicates where guards are employed (on the USAID compound and or in the Public Access Control (PAC) area); also indicates: whether guards have been provided a written set of guard orders covering both routine and emergency duties for each guard position; whether a copy of the guard orders has been provided to the USO other assigned responsibilities)) by the RSO; the number of guards available by shifts (e.g., number of hours of guard coverage at each position), supervisory responsibility, static positions, emergency response patrols; whether guard force has received adequate security procedure training from the RSO, specifically, do the guards know and carry out their emergency lock-up functions and

c. USAID/Staff Warden System: (Indicates if: A system exists to conduct routine checks of security doors to determine if the locks will engage, establishes individual responsibility for emergency locking of forced entry locks; also includes plans for bomb searches, evacuation, and movement of personnel to the safehaven; also indicates if the USAID staff is trained in their routine and emergency duties and whether drills fire, bomb, safehaven, evacuation) are routinely conducted)

d. U.S. Control of USAID Office: (Indicates whether: U.S. control of the USAID office space is constantly maintained, i.e., any time in which personnel are inside the USAID office space, a U.S. staff member is present and responsible for the security of the facility)

e. Key Control: (Indicates if the USAID office is locked by a U.S. staff member, if keys to the facility are maintained at the Chancery or other location designated by the RSO, and location/storage of any other duplicate keys)

f. Standard Operating Procedure (SOP): (Indicates if a security SOP containing both routine and emergency duties and responsibilities is published. SOP should: include duties and responsibilities of the USAID staff; visitor escort requirements and handling of National Security Information and Limited Official Use information; emergency duties identified in the SOP affix responsibilities for securing and or destroying classified and LOU material. It also should include the conditions for and the specific procedures of an evacuation, the fire plan, bomb threat plan, bomb search plan, and the alarm signal meanings).

g. Accountability of Security Equipment: (Indicates if the accountability and maintenance of security equipment has been assumed by USAID)

h. OPSEC: (Indicates if the USAID has an OPSEC program and whether the senior USAID official has designated a U.S. direct-hire employee, in writing, as the OPSEC focal point)

i. ADP Security: (Indicates if ADP equipment is used for processing of classified material; provides name and nationality of ADP systems manager; indicates if equipment is protected from theft; also includes other data pertaining to ADP systems as necessary)

C. INFORMATION SECURITY

1. Certification: (Indicates whether facility is certified for overnight or duty hour only storage of classified material)

2. Storage Vault: (Indicates whether: vault is constructed to standards, vault door meets standards (contained in Confidential 1988 State Cable 072432), type of alarm, entry/exit verification device, response force (time, composition, number responding or 24-hour US presence), and type of container used. Also indicates classification level of classified stored and volume by linear foot (1 drawer is 2 linear feet))

3. Access: (Indicates if: classified material is maintained in authorized areas, stored in the authorized areas only, and transported (within, into, and out of the building) in accordance with Confidential 1987 State Cable 324710 and 5 FAM 900; whether classified material is transmitted between the Embassy and USAID facility by a USDH in a USAID official vehicle)

4. Preparation/discussion: (Indicates if facility is authorized for preparation or discussion of classified material. Also indicates what type of equipment is used for preparation of classified material)

5. Destruction: (Indicates whether destruction of classified is conducted at facility and type of device, e.g., shredder, used and by whom)

6. Inspections: (Indicates if facility is inspected by RSO or others during duty hours or after duty hours)

7. Combinations: (Indicates whether combinations are stored at Chancery)

8. Security Violation Program: (Indicates how many violations issued to USAID in the past year; compliance with Uniform Security Regulations regarding security violations, etc.)

9. Marking: (Indicates compliance with 5 FAM 930, Marking of Classified Documents, i.e., indicates percentage of overall classified holdings reviewed, amount of and type of non-compliance noted (overall document marking, paragraph marking, downgrading instructions, original/derivative classification used appropriately)

10. Classification Guidance: (Indicates whether there is USAID and/or post-provided written guidance on type of information that requires classification)

D. ARMORED VEHICLES

1. Heavy Armored Vehicles: (Indicates how many HAV's are at post, how they are used, and by whom; whether the vehicle is kept under cover when not in use; indicates any specific problems encountered by post, e.g., any maintenance problems; whether the vehicle operational; current odometer reading and a general statement regarding apparent condition of the vehicle, etc.)

2. Light Armored Vehicles: (Indicates number of LAV's at post, how they are used, and by whom; specific problems; whether there is a need for on-site armoring)

3. Shuttle System: (Indicates if there is a post mandated home/work shuttle system requiring armored vehicles. Also indicates if the senior USAID Officer has a HAV or LAV)

4. Drivers: (Indicates if the RSO has provided security training to the drivers of HAVs and LAVs)

5. Communications: (Indicates whether HAVs, LAVs or other USAID motor pool have mobile radios (specifies number of vehicles with mobile radios))

E. RESIDENTIAL SECURITY

1. Local RSO Policy: (Includes level of security required for the post by RSO based on threat assessment and RSG handbook requirements)

2. Program Implementation: (Contains a statement whether the senior AID official's residence and all other AID residences are basically equal in protection afforded to other post personnel and whether they are in compliance with DOS dictates; if not, any problems)

3. Program Support: (Indicates whether USAID requests for residential security upgrades and/or funding are forwarded directly to the RSO with an information copy to IG/SEC)

4. Contractors: (Residential security equipment requirements for contractors are funded through the applicable contract; also includes a brief description of protection afforded or needed for contractor residences, etc.)

5. Residence Policy: (Indicates policy regarding use of single family homes, cluster housing, apartments; indicates USAID and post policy regarding acquisition of residences, e.g., LQA, USAID lease, USAID ownership; indicates number of residences occupied by USAID U.S. direct hire at post)

6. Sampling of USAID Residences:

a. Guards: (Indicates whether guards are assigned to residential properties for AID personnel; provides average number of guards per property per shift times; emergency response patrol available; local police response to incidents, etc.; includes number of guards assigned to USAID residences)

b. Fence: (Indicates type of fence/wall or other property delineation in use, etc.)

c. Building Exterior: (Indicates adequacy of doors, grillwork, and locks, etc.)

d. Alarms: (Describes intrusion alarms available for residences; in use; operable, describes where the master control panel is located)

e. Safe Area: (Indicates if a safe area is available to families; include equipment and facilities available; can all household personnel reach the safe area in a safe manner; interior grillwork gates, etc.)

f. Communications: (Indicates if a radio and/or a working telephone is available in the residence and in safe room; indicates whether there are any communications problems)

F. PERSONNEL SECURITY

1. U.S. PSCs: (Indicates that clearances are/are not up to date for all U.S. PSC employees)

2. FSNs: (Indicates whether clearances are up to date for FSN employees)

3. LOU Certification: (Indicates whether a record of LOU certification specifying type of LOU material (subject matter) and length of certification is in the appropriate personnel file)

4. Other: (Indicates if pre-employment certifications and updates are carried out and current)

G. SECURITY TRAINING AND AWARENESS

1. USO: (Indicates if the USAID Unit Security Officer has received adequate training from the Regional Security Officer (RSO))

2. Arrival Briefings: (Indicates if newly assigned, TDY, dependents, and contractors receive a security awareness briefing from the RSO and/or USO upon arrival at post; indicates whether content of briefing covers post-specific threat considerations on terrorist activities, residential and street crime precautions)

3. Periodic Security Training: (Indicates if periodic security awareness briefings covering counterintelligence and information security are given; indicates an evaluation of USAID counterintelligence program (awareness and effectiveness); includes a review of the USAID records reflecting employee attendance at security awareness sessions)

H. INCIDENT REPORTING:

1. Incidents: (Indicates whether there have been terrorist and criminal incidents (within past year) affecting the USAID as defined in Chapter 23)

2. Reporting: (Indicates whether incident reports are forwarded to IG/SEC in accordance with Chapter 23)

PART III

SUMMARY OF EXHIBITS

(summary of all exhibits attached)

EXHIBITS

o - Maps

o - Compound and Site Plans

o - Floor Plan(s)

o - Photographs

o - Security Equipment Inventory

o - Other (as needed - may include: Bill of Materials required by recommendations, Door/Window Worksheet, Specifications as required to meet DOS standards).

ATTACHMENT 22B

FORMAT FOR INITIAL USAID RESPONSE TO Office of Security INSPECTION REPORT

SUBJECT: Office of Security INSPECTION OF USAID/_____, (MONTH & YEAR)

Subject report was received on _____. The following is the status of actions taken to implement the recommendations contained therein. The status of each recommendation listed below is keyed to the Summary of Recommendations, paragraphs ___ to ___ , Part I of subject report.

CHAPTER 23

USAID INCIDENT REPORTING

23A. Purpose

1. This chapter establishes the requirement for USAID reporting of terrorist and criminal incidents affecting AID employees, contractors and their dependents to IG/SEC This reporting requirement is exclusive of notifications to the AID Washington Duty Officer.

2. The report procedure ensures that the Administrator and other senior AID officials are kept informed of terrorist and criminal incidents which affect AID personnel.

3. The information is used by IG/SEC to determine personnel and facility security requirements at each post.

23B. Applicability

This reporting requirement is applicable to all AID overseas activities.

23C. Serious Incident Reporting

1. Serious incidents are defined as those which effect the operational status of the USAID. Such incidents may include:

a. The USAID office building has been attacked or sustained damage.

b. USAID personnel have been taken hostage, or injured or killed in other than under accidental circumstances.

2. Serious incidents include, but are not limited to terrorism, mob violence, bombings, attack or threat of attack against USAID facilities, any USAID contractor facility or project site, or residence of USAID personnel.

3. When a serious incident occurs, immediate telephonic notification to the AID Washington Duty Officer is required. The AID/Washington Duty Officer will in turn notify the IG/SEC Duty Officer. A follow-up telegram must be forwarded to IG/SEC within one work day after occurrence of the event.

23D. Other Incident Reporting

Other incidents are defined as those which do not directly affect USAID operations. These include crime, harassment, vandalism, or similar occurrences. A telegram or memorandum reporting the incident is to be forwarded to IG/SEC within five work days after occurrence of the event.

23E. Report Content

Telephonic, telegram, and memorandum reports will include a summary of the incident; date and local time incident occurred; location of affected facilities; type of incident; number, identification and affiliation of personnel affected by incident; effect of incident on USAID operations; identification of damaged equipment and estimated cost and time to repair/replace; response of host government forces.

23F. Report Distribution

Reports are required whether or not the RSO/PSO has filed a report on the incident. Reports in telegram form should cite IG/SEC as the addressee. Memorandums should be forwarded to Office of Security, SA-16, Room 415, Washington D.C. 20523-1604. A courtesy copy of all written reports should be forwarded to the RSO/PSO.