



# Department of Defense INSTRUCTION

NUMBER 5210.84

January 22, 1992,

---

---

Administrative Reissuance Incorporating Change 1, October 15, 1996

ASD(C3I)

SUBJECT: Security of DoD Personnel at U.S. Missions Abroad

References: (a) Public Law 99-399, "Omnibus Diplomatic Security and Antiterrorism Act of 1986"

- (b) *DoD Instruction 5105.57, "Procedures for the U.S. Defense Representative (USDR) in Foreign Countries," December 26, 1995*
- (c) *DoD 7750.5-M, "DoD Procedures for Management of Information Requirements," November 1986*

## 1. PURPOSE

This Instruction:

1.1. Disseminates the Memorandum of Understanding (MOU) between the Department of Defense and the Department of State on diplomatic security at United States missions abroad (enclosure E1.), and the Attorney General memorandum for the Federal Bureau of Investigation (FBI) supervision and conduct of espionage investigations of all U.S. personnel assigned to these missions (enclosure E2.).

1.2. Designates the Director, Defense Intelligence Agency (DIA), as the DoD Executive Agent for diplomatic security matters addressed in this Instruction *for all noncombatant DoD elements operating under the authority of the Chief of Mission (examples include, but are not limited to, Defense Attache' Offices and Security Assistance Organizations).*

## 2. APPLICABILITY

2.1. This Instruction applies to the Office of the Secretary of Defense (OSD), the

Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Reference (a) is the statutory basis for the authority of the Secretary of State to provide for the security of U.S. Government personnel on official duty abroad (other than those personnel under the command of the U.S. area military commander) and their accompanying dependents.

### 3. POLICY

In accordance with reference (a), it is DoD policy to cooperate, to the maximum extent possible, with the Secretary of State on the security of U.S. missions abroad, and with the Attorney General on espionage investigations of U.S. personnel at U.S. missions to ensure an effective diplomatic security, counterintelligence, and antiterrorism program.

### 4. RESPONSIBILITIES

4.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall have the primary responsibility for counterintelligence and security countermeasures described in this Instruction.

4.2. The Director, Defense Intelligence Agency as the DoD Executive Agent for diplomatic security matters addressed in the agreement shall monitor the compliance with this Instruction by DoD personnel.

4.3. The Chairman of the Joint Chiefs of Staff shall coordinate implementation of this Instruction as it applies to the combatant commanders and coordinate with the OSD, the DIA, and other DoD Components, as appropriate.

4.4. *The United States Defense Representative shall:*

4.4.1. *In accordance with reference (b), implement this Instruction in his or her respective geographic areas of responsibilities.*

4.4.2. *Coordinate with the Director, DIA on issues addressed in the Memorandum of Understanding and notify, through established channels, the DoD Executive Agent of any deficiencies in the security support received by DoD elements*

*under his or her responsibility. A copy of the communique' outlining the issue or problem shall be sent by the USDR to OASD(SO/LIC) and Principal Director, Information Warfare, Security, and Counterintelligence, OASD(C31).*

4.5. *The Heads of the DoD Components shall:*

4.5.1. *Implement this Instruction in their Components.*

4.5.2. *Coordinate with the USDR regarding issues addressed in the agreement and guidelines.*

## 5. PROCEDURES

5.1. The U.S. Defense Representative (USDR) is the in-country representative of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Commander of the Unified Command for coordination of security matters for all in-country noncombat DoD elements (i.e., those DoD personnel and organizations not assigned to, or attached to, and under the command of a combatant commander). The USDR shall act as the DoD's single point of contact for security issues relating to the MOU (enclosure E1.).

5.2. Enclosure E2. describes FBI investigative responsibility for violation of espionage laws by U.S. persons abroad. This requires all Agencies and Departments to immediately report to the FBI information or allegations of U.S. persons in violation of espionage laws and allows each Agency or Department to use internal procedures for opening investigations to determine when reporting is required. The DIA, as the DoD Executive Agent, will immediately notify the appropriate DoD Component, or Component investigative agency, upon receipt of information covered under the guidelines for appropriate action.

## 6. INFORMATION REQUIREMENTS

The reporting requirement listed in Section 5.2. of this Instruction is exempt from licensing in accordance with paragraph E.4.g. of DoD 7750.5-M, "Procedures for Management of Information Requirements.

7. EFFECTIVE DATE AND IMPLEMENTATION

This Instruction is effective immediately. Forward one copy of implementing documents to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence within 120 days; forward one copy of changes to implementing documents within 60 days of their publication.



DUANE P. ANDREWS  
Assistant Secretary of Defense  
(Command, Control, Communications  
and Intelligence)

Enclosures - 2

1. Memorandum of Understanding Between the Department of State and the Department of Defense on Overseas Security Support
2. Attorney General Guidelines for FBI Supervision or Conduct of Espionage Investigations of U.S. Diplomatic Missions Personnel Abroad

E1. ENCLOSURE 1

MEMORANDUM OF UNDERSTANDING  
BETWEEN  
THE DEPARTMENT OF STATE  
AND THE  
DEPARTMENT OF DEFENSE  
ON  
OVERSEAS SECURITY SUPPORT

The Departments of State and Defense agree to the following provisions regarding overseas security services and procedures, in accordance with the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399).

I. AUTHORITY AND PURPOSE

The Omnibus Diplomatic Security and Antiterrorism Act of 1986, hereafter referred to as the Omnibus Act, requires the Secretary of State, in consultation with the heads of other Federal Agencies having personnel or missions abroad, where appropriate and within the scope of resources made available, to develop and implement policies and programs, including funding levels and standards, to provide for the security of United States Government operations of a diplomatic nature. Such policies and programs shall include:

(1) Protection of all United States Government personnel on official duty abroad (other than those personnel under the command of a United States area military commander) and their accompanying dependents, and,

(2) Establishment and operation of security functions at all United States Government missions abroad, other than facilities or installations subject to the control of a United States area military commander.

In order to facilitate the fulfillment of these requirements, the Omnibus Act requires other Federal Agencies to cooperate, to the maximum extent possible, with the Secretary of State through the development of interagency agreements on overseas security. Such Agencies may perform security inspections; provide logistical support relating to their differing missions and facilities; and perform other overseas security

functions as may be authorized by the Secretary.

## II. TERMS OF REFERENCE: (Alphabetical Order)

Assistant Secretary of State for Diplomatic Security (DS): The office in the Department of State responsible for matters relating to diplomatic security and counterterrorism at U.S. missions abroad.

Combatant Commander: A commander-in-chief of one of the Unified or Specified Commands established by the President. For purposes of this MOU, it is the combatant commander-in-chief with geographical area of responsibility (EUCOM, PACOM, LANTCOM, CENTCOM, and SOUTHCOM). The combatant commanders' duties include security responsibilities for military personnel (and dependents) performing strictly military functions, not otherwise assigned to the Chief-of-Mission.

Consult; Consultation: Refers to the requirement to notify all concerned parties of specific matters of mutual interest prior to taking action on such matters.

Coordinate; Coordination: Refers to the requirement to notify all concerned parties of specific matters of mutual interest and solicit their agreement prior to taking action.

Controlled Access Areas (CAA): Controlled access areas are specifically designated areas within a building where classified information may be handled, stored, discussed, or processed. There are two types of controlled access areas: core and restricted. Core areas are those areas of the building requiring the highest levels of protection where intelligence, cryptographic, security and other particularly sensitive or compartmentalized information may be handled, stored, discussed, or processed. Restricted areas are those areas of the building in which classified information may be handled and stored. Classified discussions are permitted but may be limited to designated areas, depending on the technical security threat.

Defense Components/Defense Component Headquarters: Those DoD organizations which have activities located overseas that fall under the control of the Chief of Mission. Examples include: the Defense Intelligence Agency (DIA) and Defense Security Assistance Agency (DSAA).

Deputy Under Secretary of Defense for Security Police (DUSD(SP)): The policy officer of the Department of Defense responsible for matters relating to security and counterintelligence.

Diplomatic Security Service (DSS), Department of State: The offices of the Department of State responsible for the development, coordination and implementation of security policies and programs domestically and at U.S. missions abroad.

DoD Executive Agent: The Directorate for Security and Counterintelligence, Defense Intelligence Agency (DIA/OSC), has been designated as the office of primary responsibility for DoD, for matters covered by this MOU.

Emergency Action Committee (EAC): An organization established at a Foreign Service post by the Chief of Mission or principal officer, for the purpose of planning and coordinating the post's response to contingencies.

Foreign Service National (FSN): Foreign Service National (FSN) employees are foreign nationals who provide clerical, administrative, technical, fiscal and other support at Foreign Service posts abroad. FSN means an employee of any foreign service-related mission/program/activity of any U.S. Government Department or Agency overseas establishment including, but not limited to, State, AID, USIA, Commerce, Agriculture, Peace Corps, Department of Defense, (exclusive of consular agents) who is not a citizen of the United States. The term includes Third Country Nationals (TCN's). A TCN is an individual who is employed by a U.S. mission abroad and is neither a citizen of the United States nor of the country to which assigned for duty.

Non-standard Security System: Those items of security equipment which are not in the DS inventory and are not maintainable by DS personnel.

Overseas Security Policy Group (OSPG): The Overseas Security Policy Group develops, coordinates and promotes uniform policies, standards and agreements on overseas security operations, programs and projects which affect U.S. Government civilian agencies represented abroad. The primary functions of the OSPG or subgroups shall be to formulate and develop overseas security policies and guidance for official civilian missions. Implementation of policies adopted by the OSPG or by any Agency of the Federal Government represented at an overseas mission shall be the responsibility of appropriate officials of that Agency.

Post Defense Component Office: DoD offices that fall under the control of the Chief of Mission. The following offices, although only a partial listing, are examples: Defense Attached Offices (USDAOs), Joint U.S. Military Aid Groups (JUSMAGs), Joint U.S. Military Assistance Advisory Groups (JUSMAAGs), Joint

U.S. Military Missions, U.S. Military Missions (MILMISH), Military Assistance Advisory Groups (MAAGs), Military Liaison Offices (MLOs), Offices of Defense Cooperation (ODCs), Offices of Defense Representative (ODRs), Offices of Military Cooperation (OMCs), Security Assistance Offices (SAOs), Security Assistance Technical Assistance Field Teams (TAFTs), Select Defense Intelligence Agency Liaison Offices (DIALOs), U.S. Defense Liaison Offices (USDLOs), U.S. Liaison Offices (USLOs), U.S. Military Groups (MILGPs), U.S. Military Training Missions (USMTMs), U.S. Mutual Defense Assistance Office (MDAO).

Regional Security Officer (RSO): The RSO is a U.S. Foreign Service security officer serving abroad at an embassy or consulate who is responsible, through the chain of command to a Chief of Mission, for implementing and managing the Department's overseas security programs. The specific geographical regions for which RSOs have responsibility may include one or more Foreign Service posts.

Sensitive DoD Operational Programs or Activities: Those undertakings by a local Defense Component office which are mandated by DoD, or national-level authorities, and which involve sensitive national defense or national security information or matters. Examples would include: information regarding intelligence activities, sources or methods; national defense plans or contingencies; special access programs, etc.

Standard Security Equipment and Systems: Security equipment normally in the DS inventory and maintainable by DS personnel.

### III. GENERAL ISSUES

#### A. EXISTING POLICY

Nothing in this agreement shall derogate from or be construed to conflict with the authorities and responsibilities of the Secretary of State, or the Chief of Mission as described in the Omnibus Act (P.L. 99-399), the Foreign Service Act of 1980 (P.L. 96-465) and NSDD-38. The following existing agreements are appended to this MOU and remain in effect between the Departments of State and Defense, to the extent that they do not conflict with this MOU.

1. MOU between the Departments of State and Defense on Utilization and Support of Marine Security Guards, dated December 15, 1986.



2. MOU between the Naval Security and Investigative Command, Department of the Navy and the Diplomatic Security Service, Department of State relating to the Investigation of Criminal Counterintelligence Matters dated, 28 March 1988.

3. MOU between the Department of State and the Department of the Navy Concerning the Use of Naval Support Unit Personnel Assigned to the Department of State's Security Program, dated December 11, 1978.

4. DOS-DIA Agreement Regarding Support for TEMPEST Personal Commuters and Classified Information Handline Systems, incorporating the DOS-DIA Interagency Control Document (ICD) of 9 Feb 1988.

5. STATE AIRFRAME A-41, United States Policy with Regard to Local Guard Forces (LGF) Use by Diplomatic Missions.

#### B. ISSUES NOT COVERED

Should a particular security issue which is not covered in this MOU develop at a U.S. mission abroad, the interested officials, with the concurrence of the Chief of Mission, will refer the matter to the Department of State and, through the established chain of command, to the DoD Executive Agent for further consideration and subsequent policy guidance.

#### C. CONFLICTS AT POST

Should a conflict arise at post between the Defense Component office and the RSO concerning the substance or interpretation of this MOU, the interested officials will refer the matter to the Chief of Mission, through the post Emergency Action Committee (EAC). Before making any decision, the COM may elect to seek information and recommendations from the Department of State, Director of the Diplomatic Security Service (DSS) and, through the established chain of command, from the DoD Executive Agent in Washington, DC.

#### D. EXEMPTIONS

Certain DoD programs, which come under Chief of Mission authority, because of their sensitivity (as defined in Section II) shall be exempt, on a case-by-case basis, from the requirements and standards of this MOU. These programs will be separately

identified and coordinated in writing between DUSD(SP) and DS.

#### IV. PHYSICAL TECHNICAL AND PROCEDURAL SECURITY ISSUES

##### A. STANDARDS

(1) DS has the responsibility for developing and issuing physical, technical, and procedural security standards, in coordination with the members of the OSPG, and identifying approved security equipment which will enhance the security of all employees of the foreign affairs agencies and all new and existing installations at U.S. missions abroad.

(2) It is the policy of the Department of State to accord security protection on an equitable basis to all U.S. citizen employees of U.S. missions abroad. Any differences in the level of security provided to individuals or categories of employees at post must be based on specific higher threat levels placed on those employees and must be recommended by the post Emergency Action Committee.

(3) With regard to the security afforded to sensitive DoD operational programs and activities, it falls to the local Defense Component office at post to comply with established security program requirements. DoD agrees to comply with DS minimum security standards. If a local Defense Component office requests additional security measures beyond the established minimum level, it will coordinate all requests with the post RSO. If the RSO and the local Defense Component office cannot agree on the level of upgrade requested, they will refer the disagreement, through the Chief of Mission, to the Department of State and, through the established chain of command, the DoD Executive Agent in Washington, DC and request resolution of the matter. The additional costs associated with approved security upgrades will be borne by the local Defense Component office through established funding mechanisms. For sensitive DoD operations, the DoD Executive Agent will provide the DS with copies of all applicable DoD Component security requirements which exceed DS standards.

(4) Existing physical and technical security standards may be modified, whenever improved deterrents are identified. Physical and technical security equipment will undergo certification testing by U.S. Government Agencies and commercial testing laboratories that have been approved by DS. Testing will be done in accordance with DSS-approved test procedures and performance criteria, to ensure that such equipment conforms to established physical security standards.

(5) a. When existing Defense Component office space at post must be relocated, every effort must be made to obtain new space that meets current security standards. If the relocation requires moving to a separate facility outside the post chancery building, every effort will be made to locate a newly constructed facility or an existing building that meets current security standards. If security standards cannot be met in new space or in a proposed new building, the Chief of Mission and the Defense Component headquarters must be informed and a waiver must be approved by the Director of the Diplomatic Security Service (or designee) before a new facility can be leased or constructed.

b. When the Department of State mandates that post Defense Components be moved to a proposed new facility, yet that facility does not meet all current security requirements, the RSO, working with appropriate DoS offices (e.g., A/FBO), will prepare the required waiver package with input from the Defense Component and submit it formally to the Director of the Diplomatic Security Service through the Chief of Mission.

c. When the Department of Defense requests that a post Defense Component relocate to a new facility, yet that facility does not meet all current security requirements, the DoD Executive Agent will prepare the required waiver package with input from the post Defense Component, the RSO, and other appropriate DoS elements. The waiver package will be submitted to the Director of the Diplomatic Security Service, through the Chief of Mission, and according to established waiver procedures. If a waiver is denied, the DoD Executive Agent will have the opportunity to present its case to the Security Exceptions Committee which will evaluate all waiver requests, based on standards contained in the existing DS Physical Security Standards Handbook.

#### **B. SURVEYS CONDUCTED BY SECURITY PERSONNEL NOT RESIDENT AT POST:**

The DS either on its own (with prior notification to the Chief of Mission and to Defense Component Headquarters through the DoD Executive Agent) or, at the request of Defense Component officials, will be responsible for conducting complete physical, technical, and procedural surveys of all Defense Component offices attached to U.S. missions abroad. The security officer conducting the surveys will make recommendations based on standards established in the existing DS Physical Security Standards Handbook and will advise the senior official of the Defense Component

office at post, as well as the Chief of Mission, of any weaknesses or deficiencies noted in the course of such surveys. Copies of the survey will be provided to the DoD Executive Agent and DS. DoD will be afforded the opportunity to review and comment on survey recommendations which affect the operations of Defense Component office facilities.

#### C. SECURITY PROGRAM INSPECTIONS

Representatives of Defense Component Headquarters may conduct periodic or emergency surveys and inspections of their local Defense Component office facilities abroad. Such surveys and inspections may only be conducted with prior notification to the RSO at post through DSS. Further, Defense Component Headquarters and the DoD Executive Agent may review the adequacy of the local guard and residential security services provided to Defense Component offices. On such occasions, the RSO shall make available to Defense Component Headquarters inspectors such information pertaining to Defense Component offices as may be required. Defense Component Headquarters will provide the DSS and the DoD Executive Agent with copies of the final reports of security inspections made by its personnel. If additional resources are required to support DoD's findings, this determination must be referred to both Departments for further coordination. Prior to departure from the post, the Defense Component Headquarters representative conducting the inspection will review the recommendations or issues with the RSO, attempt to resolve them, and provide the RSO with a copy of the draft report. Any remaining differences in recommendations or issues which cannot be resolved at post between the inspecting Defense Component Headquarters representative and the RSO, will be handled in accordance with the procedures in Section III-C. of this agreement entitled, "Conflicts at Post".

#### D. LOCAL GUARD PROGRAM

The RSO shall establish and implement local guard procedures necessary for the security of post Defense Component official facilities and residences. The level of protection provided to the Defense Component office will comply with approved OSPG Local Guard Program standards.

#### E. RESIDENTIAL SECURITY

The RSO will establish and implement a residential security program applicable to all American personnel under the authority of a Chief of Mission. The level of protection

provided to the Defense Component office will comply with approved OSPG Residential Security standards.

#### F. ARMORED VEHICLES

On a reimbursable basis, Defense Components may arrange with DS to install light vehicle armoring to DoS specifications in local Defense Component office vehicles. The level of protection provided to the Defense Component office will comply with approved OSPG Armored Vehicle standards.

#### G. FORCED ENTRY/PENETRATION

All instances involving the physical penetration of a building, including unauthorized entry or damage to property, as well as possible compromise of classified information, will be reported by Defense Component Office personnel to the RSO and the Chief of Mission. The RSO will conduct appropriate investigations and provide the Chief of Mission and the Executive Agent with the full details of the incident, as well as any follow-up action, by telegram via the Department of State.

Suspected technical security penetrations and hazards discovered by post Defense Component personnel will be reported to the RSO for appropriate action. Reports of technical security penetrations of or hazards in post Defense Component offices will be provided expeditiously to the DoD Executive Agent by DS, under the provisions of the DCI Procedural Guide I-II-III.

#### H. STORAGE OF CLASSIFIED MATERIALS

U.S. missions will store and safeguard classified and administratively controlled materials, in accordance with DoS regulations and policies. At facilities approved for storage of classified information, the RSO will designate controlled access areas and establish supervisory controls over the distribution and storage of classified and administratively controlled materials. All Defense Component offices are subject to accreditation by DS for classified storage up to an authorized security classification level, in accordance with DoS Security Standards for the Storage of Classified information at posts abroad.

#### I. SECURITY VIOLATIONS

The RSO will implement security violation reporting procedures for Defense Component office facilities, in conformance with those specified in existing DoS regulations and policies. All classified material violations involving Defense Component office personnel will be reported directly by the RSO, through mission channels, to the DoD Executive Agent and Defense Component Headquarters for administrative or disciplinary action within thirty (30) days after the violation is discovered. Copies of these reports will also be sent by the RSO to DS.

#### J. POST TRAINING AND ORIENTATION

The RSO will include U.S. Defense Component office employees at post in training and indoctrination lectures, crisis management drills and in the dissemination of security awareness materials.

#### K. UNIT SECURITY OFFICERS

Where determined to be of practical operational value and in consultation with the RSO, a Unit Security Officer will be appointed by the Defense Component office at post. The Unit Security Officer will be responsible for the conduct of daily physical, technical and procedural security services for the Defense Component office and will assist the RSO, as requested, in DoD investigative activities. The Unit Security Officer will be trained and guided by the RSO in the execution of security functions for post Defense Component offices.

#### L. REPORTS

Copies of routine reports or correspondence pertaining to all activities conducted by or under the direction of the RSQ, dealing with the Defense Component office physical, technical, or procedural security matters, will be furnished through mission channels and DS, to the Defense Component Headquarters and DoD Executive Agent. Recommendations for correcting deficiencies as well as corrective action taken will be included in such reports. Alerts, security incidents, or notices of threats to U.S. personnel and facilities under the authority of a Chief of Mission, involving local Defense Component offices or personnel, will be provided to Defense Component Headquarters, the DoD Executive Agent, and the area Commander immediately by telegram. Similarly, Defense Component Headquarters and the DoD Executive Agent will provide copies of correspondence to DS headquarters and RSOs, when

communicating on such matters with Defense Component offices at post.

#### M. INSTALLATION AND MAINTENANCE OF SECURITY SYSTEMS

Subject to survey recommendations, DS will install standard security systems at Defense Component offices at post upon request of the DoD Executive Agent, either by using Security Engineering Officers, Seabees, or Security Engineering Contractors or other cleared American contractors. Equipment installed shall either be procured by DoD Component Offices at post or, obtained from the DS inventory. The maintenance of standard DS technical security equipment at Defense Component offices at post will be included in the DS Security Engineering Maintenance Program. The maintenance of non-standard equipment, which is not in DS inventory, will be the responsibility of the post Defense Component office. In cases where Defense Components require technical equipment which is non-standard to the DoS inventory, the local Defense Component office will procure, install and maintain the equipment at its own cost. Non-standard technical equipment will only be used if a DS Security Engineering Officer certifies that it will not interfere with any standard DoS equipment installed. The Defense Component office, with DS concurrence, may contract separately for maintenance of security systems at remote sites which require extensive maintenance of a timely and frequent nature.

#### N. REQUESTS FOR RSO ASSISTANCE/JOINT INSPECTIONS

Requests from Defense Components Headquarters or the DoD Executive Agent to the RSO for physical, technical and procedural security assistance not addressed elsewhere in this MOU will be cleared through the DSS Directorate of Overseas Operations (DS/DSS/OP). In the event of dissatisfaction with security services provided by the RSO to post Defense Components offices and when attempts to resolve problems in consultation with the RSO have failed, the post Defense Component office may bring its concerns to the Chief of Mission, through the Emergency Action Committee (EAC), in accordance with Section III C. of this MOU. The EAC may recommend to the Chief of Mission that a joint inspection of the facilities be performed by the headquarters staff of DS and representatives of the DoD Executive Agent or Defense Component Headquarters, to assess the security services being provided to post Defense Components offices.

#### O. TECHNICAL SECURITY

DS Security Engineering Officers (SEO's) will include post Defense Component offices in routine technical security countermeasures (TSCM) inspections of controlled access areas at post, where the technical threat warrants such routine inspections. DoD is responsible for the costs of TSCM inspections of Defense Component offices at posts where DS has determined that the technical threat does not warrant more frequent inspections. The Defense Component Headquarters or the DoD Executive Agent may dispatch people and equipment to post to conduct technical security inspections and investigations of post Defense Component Offices. Such activities will be coordinated in advance with DS, the RSO and the DoD Executive Agent. All information obtained from such investigations will be shared with the RSO, the Defense Component Office at post, DS and the DoD Executive Agent and reported to them following the DCI Procedural Guide I-II-III.

#### P. CONSTRUCTION SECURITY

The Department of State will provide DoD with the construction security training required to enable DoD personnel to perform construction security on non-A/FBO projects in DAO office space within U.S. missions abroad. This training will involve construction surveillance techniques and guard responsibilities. Non-A/FBO projects are those which do not substantially change the structural, mechanical, electrical, life-safety, or architectural systems within a U.S. mission abroad.

#### V. INVESTIGATIONS

##### A. GENERAL

DS has, inter alia, the responsibility for investigating: a) U.S. Citizen applicants, b) foreign national applicants, and c) employees and contractors of DoD at U.S. missions abroad. All requests for investigations, except routine embassy source and police checks originated by the post Defense Component office, will be channeled through DSS to the RSO, or processed as specified in separate agreements. Requests for routine embassy source checks may be made directly to the RSO or Post Security Officer (PSO) by the post: Defense Component office. Copies of investigative reports, contact reports and correspondence relating to investigative support of DoD matters or personnel will be furnished to the DoD Executive Agent via DSS. DoD may, at its discretion, dispatch persons from its Defense Component headquarters staff to inquire into a DoD investigative matter. All such activity will be coordinated in



advance with the Chief of Mission through the RSO and DS headquarters.

**B. U.S. CITIZEN EMPLOYEES FOREIGN NATIONAL SPOUSES & FIANCEES, AND CONTRACTORS**

(1) U.S. citizen employees, spouses and contractors of post Defense Components assigned on a permanent and temporary basis at U.S. Missions abroad may be investigated by the RSO: (a) upon the request of the Defense Component headquarters through the DoD Executive Agent and DS, or (b) at the direction of the Chief of Mission, when allegations or complaints of a security nature are received. It is DS policy that RSO's are not authorized to initiate an investigation of a U.S. citizen employee or applicant abroad without the advanced approval of the appropriate DS headquarters element. Should the Chief of Mission direct such an investigation, the RSO may proceed but must immediately notify DS of all relevant information. Prior to initiating an official investigation of any post Defense Component employee or contractor, and subsequent to preliminary inquiries of allegations or complaints, the RSO will report the case to the DoD Executive Agent, via DS, as expeditiously as possible.

(2) No U.S. citizen employee or contractor of DoD, who is the subject of an official investigation by the RSO, shall be interviewed without the approval of and instructions from Defense Component headquarters and the DoD Executive Agent through DS, unless requested by the Chief of Mission. Any time the RSO conducts a formal investigation concerning U.S. citizen employees or contractors of DoD, a full report shall be forwarded to the Defense Component Headquarters and the DoD Executive Agent via DS. Urgent matters shall be handled by telegram.

(3) Investigations of foreign national spouses or proposed foreign national spouses of U.S. citizen employees will be conducted consistent with State Department personnel policies, as staged in Volume Three of the Foreign Affairs Manual (3 FAM). Such investigations may be supplemented by DoD, in accordance with established personnel security investigation procedures, when deemed in the interest of national security.

**C. FOREIGN NATIONAL EMPLOYEES AND CONTRACTORS**

(1) The RSO and the Defense Component office at post will ensure that all foreign nationals proposed for contractual status or employment are investigated, in accordance with established procedures and that the RSO will issue a certification for

employment in each approved case. Investigations should be completed prior to employment or execution of a contract. However, such persons may be employed on an interim basis, upon the completion of a satisfactory local investigation and temporary certification by the RSO. Continued employment will be contingent upon satisfactory results of a completed investigation. Foreign National employees and contractors are to be re-investigated and certified every five years.

(2) Allegations of misconduct against foreign national employees and contractors will be investigated by or under the direction of the RSO. Detailed reports of such investigations shall be forwarded to the DoD Executive Agent through DS. The results of such investigations shall be the basis for a determination by the RSO of corrective action to be taken, subject to the concurrence of the Chief of Mission. The RSO will refer to Defense Component Headquarters through DS and the DoD Executive Agent, any cases for which the Chief of Mission believes a decision should be made by Defense Component Headquarters.

(3) The RSO and the Defense Component office at post will ensure that every foreign national, whose position at post requires access to administratively controlled information, is properly investigated and certified,

(4) Security checks and/or investigations of domestic staff of U.S. Defense Component office employees will be conducted consistent with post policy.

## VI. TRAINING

A. DS will sponsor DoD Executive Agent personnel for appropriate security-related training offered by the Diplomatic Security Training Center (DS/TC), commensurate with the security clearance level and the need-to-know of the applicant. Such sponsorship is subject to course quota availability.

B. The DoD Executive Agent will sponsor DS personnel for appropriate security-related training, commensurate with the security clearance level and need-to-know of the applicant. Such sponsorship is subject to course quota availability.

## VII. BUDGET AND REIMBURSEMENT

A. The Department of State and the Department of Defense will fund diplomatic

security programs as specified in the Security Funding Matrix (Appendix A). DoS will fund, within funds available, standard DS security equipment and support that is commensurate with established threat levels. DoD Defense Components will fund non-standard DS security equipment and support which exceeds established threat levels. DoD Defense Component funding will be administered directly between the Defense component and the contract supporting this service or support.

B. All DS resource planning will be conducted in consultation with agencies represented at U.S. missions abroad, in order to provide an annual consolidated overseas security budget proposal.

C. Defense Component headquarters, utilizing its authority to protect its personnel and operations under the Internal Security Act of 1950 (50 U.S.C. 797), interalia, will authorize local Defense Component offices to reimburse the Department of State for security services rendered to local Defense Component offices that exceed DoS funding allocations, upon formal notification of the DoD Executive Agent by DS of the projected security program funding shortfall.

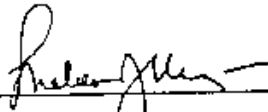
1. Whenever possible, funding shortfalls should be identified in advance of the budget execution year.

2. Reimbursement will be handled at the post level through standard procedures for reimbursement for services rendered and will be based upon actual or allocated costs of services rendered to the local Defense Component office under the aegis of the Emergency Action Committee.

VI. IMPLEMENTATION AND TERMINATION

This Memorandum of Understanding will become effective upon signature by the representatives of the Department of State and the Department of Defense named below. It will remain in force until notification by either party, sixty days in advance, of its intention to terminate the conditions of the agreement.

U.S. Department of State,  
Assistant Secretary for  
Diplomatic Security



Sheldon J. Krys

Date: 17 September 1990

U. S. Department of Defense,  
Deputy Under Secretary of  
Defense (Security Policy)



Craig Alderman, Jr.

Date: 19 August 1990

APPENDIX A

DEPARTMENT OF STATE AND DEPARTMENT OF DEFENSE  
SECURITY FUNDING MATRIX

Delineation of Funding Responsibilities in MOU

<u>Program</u>	<u>DoD</u>	<u>DoS</u>
<u>Armored Vehicles (FAV &amp; LAV)</u>		
Procurement, armoring & transportation	X	
Inspection	X	
<u>Local Guards (See Note)</u>		
		X
<u>Residential Security</u>		
Purchase, install and maintain residential upgrades		X
<u>Physical Security, Non-Residential Buildings</u>		
Purchase, install and maintain DS standard equipment for non-residential upgrades		X
Purchase, install and maintain non-standard equipment for non-residential upgrade	X	
Surveys of DoD facilities		X
<u>Technical Security</u>		
Purchase, install and maintain DS standard equipment to meet DS security standards		X
Purchase, install and maintain non-standard equipment or equipment exceeding DS standards	X	
Maintain equipment at remote DoD sites for which DoS cannot provide timely service Surveys of DoD facilities		X

NOTE: Local Defense Component offices are authorized to reimburse DS for the local Defense Component office's share of costs, which exceed the approved field budget plan for a post. LGP costs include roving patrols, static guards and counter surveillance teams where appropriate. Cost share determinations will be based upon the actual or allocated cost of services rendered to the local Defense Component office.

## Delineation of Funding Responsibilities in MOU

<u>Program</u>	<u>DoD</u>	<u>DoS</u>
<u>Technical Countermeasures</u>		
Routine TSCM inspections of DoD controlled access areas.		X
TSCM inspections of DoD controlled access areas which exceed standard determined by post threat level	X	
<u>Transit Security</u>		
Secure shipment, storage and surveillance of construction materials for FBO projects at DoD controlled access areas		X
Secure shipment, storage and surveillance of construction materials for non-FBO projects at DoD controlled access areas	X	
Secure shipment, storage and surveillance of non-classified sensitive materials unrelated to construction projects	X	
<u>Construction Security</u>		
Surveillance and guards for FBO projects at DoD controlled access areas		X
Surveillance and guards for non-FBO projects at DoD controlled access areas	X	
<u>Training and Orientation</u>		
At-post security training specifically requested by DoD and restricted to their personnel only, both US and FSN	X	
Washington-based security training offered by DS and DS/TC	X	
<u>Investigations</u>		
Overseas background investigations (US & FSN) of prospective DoD employees at US missions abroad	X	
Investigations of foreign national spouses		X

## E2. ENCLOSURE 2

### Attorney General Guidelines for FBI Supervision or conduct of Espionage Investigations of U.S. Diplomatic Missions Personnel Abroad

Section 603 of the Intelligence Authorization Act for Fiscal Year 1990 clarifies the responsibilities of the Federal Bureau of Investigation and other Departments and Agencies of the United States with regard to the investigation of suspected violations of the espionage laws by personnel (including foreign service nationals) employed by, or assigned or attached to, United States diplomatic missions abroad ("U.S. personnel"). These guidelines, developed in consultation with affected Departments and Agencies, are intended to implement that section and provide for appropriate coordination, reporting and investigation concerning such matters.

#### I. REPORTING TO THE FBI BY OTHER DEPARTMENTS AND AGENCIES

All Departments and Agencies shall report immediately to the FBI any information, allegations, or circumstances involving any "U.S. personnel" who may be engaged in violations of the espionage laws of the United States. Departments and Agencies with law enforcement investigative authorities may rely upon their internal guidelines or procedures that establish predicates for opening investigations concerning suspected violations of the espionage laws of the United States as a threshold for determining when a report to the FBI is required under these guidelines. Departments and Agencies that do not have such authority should report to the FBI whenever sufficient information is available to indicate any "U.S. personnel" at a particular diplomatic mission (whether or not specifically identified by name) may be engaged in such activities.

At minimum, it is contemplated that the FBI will be advised at once whenever any Department or Agency identifies any particular "U.S. personnel" as possibly having violated the espionage laws of the United States. Information concerning routine screening or suitability matters or violations of security regulations or procedures by "U.S. personnel" need not be reported unless indications of connections to foreign government entities that may involve espionage are developed. Unsubstantiated, non-specific information also need not be reported unless there

appears to be a connection between "U.S. personnel" and possible espionage.

Whenever there is any question concerning whether information should be reported to the FBI, informal consultations should take place between the FBI and Department or Agency representatives at the headquarters level. Issues unresolved by these informal consultations shall be directed to the Office of Intelligence Policy for resolution in consultation with the Internal Security Section of the Criminal Division. Thereafter, any continuing concerns by Departments and Agencies may be raised with the Attorney General for resolution.

All reporting under these guidelines shall be made under the secure means of communication that is available.

## II. CONDUCT AND SUPERVISION OF INVESTIGATIONS

As a general matter, the FBI has overall responsibility for the conduct of espionage investigations at United States embassies and other diplomatic establishments outside the United States. In furtherance of this responsibility, the FBI shall supervise the conduct of, or conduct itself as explained further below, all investigations of violations of the espionage laws of the United States by any "U.S. personnel."

Whether FBI personnel should actually conduct or supervise such an investigation is a matter for the FBI to determine, in appropriate consultation with relevant Departments and Agencies, depending upon the particular facts and circumstances of each case. Any decision to send FBI personnel abroad for such purposes shall be coordinated with relevant Agencies and Departments and approved by the Director of Central Intelligence as required by applicable guidelines and procedures and is subject to the approval of the Secretary of State and the Chief of Mission consistent with 22 U.S.C. 4802(b) (1) and 3927.

Whenever the FBI determines it to be appropriate and desirable, investigative capabilities, resources and lawful techniques available to other Departments and Agencies, particularly those whose employees or contractors may be suspected of an espionage violation, shall be utilized in furtherance of such an investigation. In these instances, the FBI shall supervise the activities of the investigating Departments or Agencies and shall be informed contemporaneously of all significant developments. Any assistance requested or provided under this authority shall be consistent with the respective authorities and responsibilities of the Departments and Agencies.



In appropriate cases, the FBI may establish an investigative team under the supervision of FBI personnel and including investigative or other relevant officials of other Departments and Agencies.

Any issues or concerns with respect to the FBI's exercise of its authority in particular investigations shall be directed to the Internal Security Section of the Criminal Division for resolution. Thereafter, any continuing concerns by Departments or Agencies may be raised with the Attorney General for resolution.

### III. MISCELLANEOUS PROVISIONS

A decision by the FBI to terminate or not to pursue an espionage investigation in a particular case does not preclude further investigation by appropriate Departments and Agencies provided that such activities are conducted in consultation with the FBI and any information concerning possible violations of the espionage statutes that may be subsequently developed is reported immediately to the FBI.

Nothing in these guidelines shall be construed to establish any defense to any criminal, civil, or administrative action.

Nothing in these guidelines is intended to alter the responsibilities of the Director of Central Intelligence under the National Security Act of 1947 for the protection of intelligence sources and methods or under Executive Order 12333 for counterintelligence liaison with the intelligence and security services of foreign governments, or the responsibility of the Central Intelligence Agency under that Order for the coordination of counterintelligence activities abroad.

Nothing in these guidelines is intended to affect decisions by the Justice Department, in appropriate consultation with relevant Departments and Agencies, concerning the prosecution of any particular case.

Nothing in these guidelines is intended to provide the FBI with the authority to coordinate the conduct of damage assessments in connection with possible espionage violations. Departments and Agencies that conduct such assessments should recognize, however, that such assessments may have some impact upon the success of an investigation or a potential prosecution and consult with the FBI and the Department of Justice as appropriate.

Nothing in these guidelines is intended to alter any limitation placed upon the

functions of another Department or Agency and its personnel by law, executive order, regulation, or Attorney General-approved procedures or guidelines, including procedures related to the conduct of non-law enforcement counterintelligence activities outside the United States by the FBI.


Nothing in these guidelines is intended to alter obligations by agencies within the Intelligence Community to report violations of Federal statutes under section 1.7(a) of Executive order 12333 or Implementing procedures promulgated thereunder.

Nothing in these guidelines shall be construed to authorize a violation of any applicable Status of Forces Agreement (SOFA).

Nothing in these guidelines is intended to alter the statutory authority of the Secretary of State for all aspects of diplomatic security as set forth in the Omnibus Diplomatic Security and Antiterrorism Act of 1986.

Proposals to amend these guidelines shall be directed to the Office of Intelligence Policy and Review.

APPROVED:

  
\_\_\_\_\_  
Dick Thornburgh  
Attorney General

APR 17 1990

\_\_\_\_\_  
Date