

Security

**Foreign
Disclosure,
Technology
Transfer, and
Contacts with
Foreign
Representatives**

Headquarters
Department of the Army
Washington, DC
15 February 2001

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-10

Foreign Disclosure, Technology Transfer, and Contacts with Foreign Representatives

This revision--

- o Assigns the Deputy Under Secretary of the Army (International Affairs), HQDA, management oversight responsibility for the application of Army policy regarding foreign disclosure, technology transfer, and munitions license review function. Subject to the direction of the Deputy Under Secretary of the Army (International Affairs), the Deputy Chief of Staff for Intelligence will have responsibility for policy formulation and staff execution for foreign disclosure and technology transfer (para 1-5 and 1-6).
- o Describes the role foreign disclosure (to include international technology transfer) plays in facilitating international programs and in contributing to the attainment of United States National Security Strategy and National Military Strategy goals and objectives (para 2-1a and b).
- o Implements guidance contained in Department of Defense Directive 5230.20, dated 12 August 1998 (appendices J-0).
- o States that the authority for the disclosure of controlled unclassified information may be vested in the respective originators/proponents of the information (paras 1-1, 1-4a, 1-7c, and 2-8).
- o Assigns oversight responsibility for foreign disclosure training to the Deputy Chief of Staff for Intelligence (para 1-6i).
- o Incorporates new Department of Defense policy regarding Cooperative Program Personnel (paras 1-1, 1-4a (4)(d), 1-5g, and appendix O).
- o Updates the policy and procedures involving the Military Personnel Exchange Program, and Engineers and Scientists Exchange Program (appendices M and N).
- o Changes policy and procedures regarding the Foreign Liaison Officer Program (appendix K).
- o Clarifies policy regarding the assignment of administrative support personnel to foreign liaison officers (appendix K).

Effective 15 March 2001

Security

Foreign Disclosure, Technology Transfer, and Contacts with Foreign Representatives

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

History. This printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. The National Security Strategy of the United States stresses that the “imperatives of engagement” in the world is vital for our security. To achieve our security objectives, the United States must remain the preferred security partner for the community of states that shares our interests. Foreign disclosure and technology transfer are key components that contribute to the achievement of our strategy of engagement. This regulation provides policy and procedures for the disclosure of United States Army classified military information and certain controlled unclassified information to foreign governments

and international organizations; policy regarding contacts with foreign representatives; certification of foreign liaison officers, and foreign exchange and foreign cooperative program personnel to Department of the Army commands, installations, and contractor facilities for which the Department of the Army is the executive agent or has security cognizance; guidelines for foreign representative attendance at Army-sponsored meetings, conferences, and symposia; and establishment of policy, procedures, and assignment responsibilities for controlling the direct and indirect international transfer of critical military information and technology. This regulation implements the National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations, short title: National Disclosure Policy, Department of Defense Directives 2040.2, 5230.11, and 5230.20.

Applicability. This regulation applies to the Active Army, the Army National Guard of the United States, and the United States Army Reserve. It applies to all personnel involved in the foreign disclosure and technology transfer process.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence, who has the authority to approve exceptions to this regulation that are consistent with controlling laws and regulations. The proponent may delegate this authority, in

writing, to a division chief within the Office of the Deputy Chief of Staff for Intelligence.

Army management control process. This regulation contains management control provisions. The Management Control Evaluation Checklist is at appendix B.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff for Intelligence.

Suggested Improvements. Users are invited to send comments and suggested improvements on Department of the Army Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, 1000 Army Pentagon, Washington, DC 20310-1001.

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

General, page 1

Section I

Introduction, page 1

Purpose • 1–1, page 1

References • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

*This regulation supersedes Army Regulation 380-10, 30 December 1994.

Contents—Continued

Policy • 1–4, *page 1*

Section II

Responsibilities, page 4

Deputy Under Secretary of the Army (International Affairs), HQDA • 1–5, *page 4*

Deputy Chief of Staff for Intelligence (DCSINT), Headquarters, Department of the Army (HQDA) • 1–6, *page 4*

Heads of HQDA Staff Agencies and MACOM Commanders • 1–7, *page 5*

Deputy Chief of Staff for Operations and Plans (DCSOPS), HQDA • 1–8, *page 5*

Assistant Secretary of the Army (Acquisition, Logistics and Technology (ASA(ALT))) • 1–9, *page 6*

Deputy Under Secretary of the Army (Operations Research) (DUSA(OR)), HQDA • 1–10, *page 6*

Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM) • 1–11, *page 6*

Commanding General, U.S. Army Materiel Command (CG, AMC) • 1–12, *page 6*

The Judge Advocate General • 1–13, *page 7*

The Surgeon General (TSG), the Chief of Engineers (COE), and the Director, Information Systems for Command, Control, Communications and Computers (DISC4) • 1–14, *page 7*

CG, U.S. Army Criminal Investigation Command (USACIDC) • 1–15, *page 7*

Overseas major commanders • 1–16, *page 7*

Other Overseas Army Activities • 1–17, *page 7*

Chapter 2

General Disclosure Policies, Authority to Disclose, and Delegation of Authority, *page 7*

Section I

Introduction, page 7

Concept • 2–1, *page 7*

False Impression • 2–2, *page 8*

Categorization of Military Information • 2–3, *page 8*

Categories of Military Information • 2–4, *page 8*

Maximum Delegated Disclosure Levels • 2–5, *page 10*

Basic Disclosure Criteria • 2–6, *page 10*

Establishment of disclosure programs pursuant to international agreements • 2–7, *page 12*

Section II

Authority to Disclose CMI and CUI and Delegation of Disclosure Authority, page 13

CUI disclosure authority and delegation of authority • 2–8, *page 13*

CMI disclosure authority and delegation of authority • 2–9, *page 13*

Delegation of Disclosure Authority Letter • 2–10, *page 14*

Responsibilities and establishment of foreign disclosure officers • 2–11, *page 14*

Foreign disclosure channels and general decision procedures • 2–12, *page 15*

Chapter 3

Modes, Methods, and Channels for CMI Disclosures and Related Administrative Procedures, *page 16*

Section I

Procedures for Disclosure to or by Visitor, Exchange, Cooperative, and Liaison Personnel, page 16

Concept • 3–1, *page 16*

DA CMI Disclosed During Visits • 3–2, *page 16*

DA CMI disclosed to or by FLO, Foreign Exchange, and Cooperative Program personnel • 3–3, *page 17*

Documentary requests for U.S. CMI • 3–4, *page 17*

Section II

Foreign Access to Automation, page 18

Foreign access to computers and computer networks. • 3–5, *page 18*

Secret Internet Protocol Router Network (SIPRNET). • 3–6, *page 18*

Non-Secure Internet Protocol Routing Network (NIPRNET). • 3–7, *page 18*

Contents—Continued

Section III

Administrative Procedures, page 19

Concept • 3–8, *page 19*

Physically conveying CMI documentary material • 3–9, *page 19*

Recording CMI disclosure determinations and transfers • 3–10, *page 19*

Chapter 4

International Technology Transfer Program, page 23

Concept • 4–1, *page 23*

Technology Control Panel • 4–2, *page 23*

International technology transfer documentation • 4–3, *page 23*

Appendixes

A. References, *page 25*

B. Management Control Evaluation Checklist and DA Staff Assistance and Compliance Visits, *page 29*

C. Exceptions to Policy, *page 31*

D. Technology Assessment/Control Plan (TA/CP), *page 37*

E. Delegation of Disclosure Authority Letter (DDL), *page 39*

F. Summary Statement of Intent (SSOI), *page 65*

G. Frequently Asked Questions, *page 68*

H. Meetings, Conferences and Symposia, *page 71*

I. Policy and Procedures for Disclosure of CMI in Support of International Activities, *page 72*

J. DA International Visits Program, *page 76*

K. Foreign Liaison Officers, *page 86*

L. Standardization Representatives, *page 102*

M. Military Personnel Exchange Program, *page 117*

N. Engineers and Scientists Exchange Program, *page 123*

O. Cooperative Program Personnel, *page 131*

Table List

Table 3–1: Document Request Procedures, *page 20*

Figure List

Figure 2–1: Political and military criteria, *page 11*

Figure 2–1: Political and military criteria—Continued, *page 12*

Figure 3–1: Processing of request involving CMI, *page 22*

Figure C–1: Format for a request for an ENDP, *page 32*

Figure C–1: Format for a request for an ENDP—Continued, *page 33*

Figure C–1: Format for a request for an ENDP—Continued, *page 34*

Figure C–1: Format for a request for an ENDP—Continued, *page 35*

Figure C–1: Format for a request for an ENDP—Continued, *page 36*

Figure E–1: Sample format of DDL for weapons system, *page 40*

Figure E–1: Sample format of DDL for weapons system—Continued, *page 41*

Figure E–1: Sample format of DDL for weapons system—Continued, *page 42*

Figure E–1: Sample format of DDL for weapons system—Continued, *page 43*

Figure E–1: Sample format of DDL for weapons system—Continued, *page 44*

Figure E–2: Sample matrix, *page 45*

Figure E–2: Sample matrix—Continued, *page 46*

Contents—Continued

- Figure E-2: Sample matrix—Continued, *page 47*
Figure E-2: Sample matrix—Continued, *page 48*
Figure E-2: Sample matrix—Continued, *page 49*
Figure E-2: Sample matrix—Continued, *page 50*
Figure E-2: Sample matrix—Continued, *page 51*
Figure E-2: Sample matrix—Continued, *page 52*
Figure E-2: Sample matrix—Continued, *page 53*
Figure E-2: Sample matrix—Continued, *page 54*
Figure E-2: Sample matrix—Continued, *page 55*
Figure E-2: Sample matrix—Continued, *page 56*
Figure E-2: Sample matrix—Continued, *page 57*
Figure E-2: Sample matrix—Continued, *page 58*
Figure E-3: Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions, *page 59*
Figure E-3: Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued, *page 60*
Figure E-3: Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued, *page 61*
Figure E-3: Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued, *page 62*
Figure E-3: Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued, *page 63*
Figure E-3: Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued, *page 64*
Figure F-1: Summary statement of intent, *page 65*
Figure F-1: Summary statement of intent—Continued, *page 66*
Figure F-1: Summary statement of intent—Continued, *page 67*
Figure F-1: Summary statement of intent—Continued, *page 68*
Figure G-1: Frequently asked questions and corresponding answers, *page 69*
Figure G-1: Frequently asked questions and corresponding answers—Continued, *page 70*
Figure J-1: Processing of request for visit authorization (RVA) from foreign military attaches, *page 85*
Figure K-1: FLO LOA conditions and limitations, *page 92*
Figure K-1: FLO LOA conditions and limitations—Continued, *page 93*
Figure K-1: FLO LOA conditions and limitations—Continued, *page 94*
Figure K-1: FLO LOA conditions and limitations—Continued, *page 95*
Figure K-2: Sample certification, *page 96*
Figure K-2: Sample certification—Continued, *page 97*
Figure K-2: Sample certification—Continued, *page 98*
Figure K-2: Sample certification—Continued, *page 99*
Figure K-3: Establishment of FLO, StanRep and CPP positions, *page 100*
Figure K-4: Processing of FLO, StanRep, MPEP, and CPP nominations, *page 101*
Figure L-1: StanRep LOA conditions and limitations, *page 107*
Figure L-1: StanRep LOA conditions and limitations—Continued, *page 108*
Figure L-1: StanRep LOA conditions and limitations—Continued, *page 109*
Figure L-1: StanRep LOA conditions and limitations—Continued, *page 110*
Figure L-2: Sample certification, *page 111*
Figure L-2: Sample certification—Continued, *page 112*
Figure L-2: Sample certification—Continued, *page 113*
Figure L-2: Sample certification—Continued, *page 114*
Figure L-2: Sample certification—Continued, *page 115*
Figure L-2: Sample certification—Continued, *page 116*
Figure L-2: Sample certification—Continued, *page 117*
Figure M-1: Sample certification for MPEP participant, *page 121*
Figure M-1: Sample certification for MPEP participant—Continued, *page 122*
Figure M-2: Establishment of MPEP positions here, *page 123*

Contents—Continued

- Figure N-1: Sample commitment to hosp party statement-ESEP, *page 127*
- Figure N-2: Sample certification for ESEP person, *page 128*
- Figure N-3: Establishment of ESEP positions, *page 129*
- Figure N-4: Processing of ESEP nominations, *page 130*
- Figure O-1: Sample commitment to host party statement-CPP, *page 136*
- Figure O-2: Sample certification for CPP participant, *page 137*
- Figure O-2: Sample certification for CPP participant—Continued, *page 138*

Glossary

Index

RESERVED

Chapter 1 General

Section I Introduction

1–1. Purpose

This regulation provides policy and procedures for the disclosure of Army classified military information (CMI) and certain controlled unclassified information (CUI) to foreign governments and international organizations; policy regarding contacts with foreign representatives; certification of foreign liaison officers, and foreign exchange and foreign cooperative program personnel to Department of the Army (DA) commands, installations, and contractor facilities for which DA is the executive agent or has security cognizance; guidelines for foreign representative attendance at Army-sponsored meetings, conferences, and symposia; and establishment of policy, procedures, and assignment of responsibilities for controlling the direct and indirect international transfer of critical military information and technology. It delegates authority for routine foreign disclosure decisions and defines channels for resolving foreign disclosure issues.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A. Additionally, the Management Control Evaluation Checklist is provided at appendix B.

1–3. Explanation of abbreviations and terms

Abbreviations and terms used in this regulation are explained in the glossary.

1–4. Policy

a. This regulation prescribes DA policies and procedures governing the disclosure of CMI and certain CUI and contacts with foreign representatives (see glossary), as outlined below.

(1) *Disclosure of CMI.* This regulation governs the disclosure of CMI, identified herein, to representatives of foreign governments and international organizations (hereafter referred to as “foreign disclosure”). CMI is defined as information originated by or for the Department of Defense (DOD) or its departments or agencies or under their jurisdiction or control, and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL, as described in Executive Order 12958 (hereafter “CMI”). CMI may be in oral, visual, or documentary form. (See Army Regulation (AR) 380-5.)

(2) *Disclosure of CUI.* This regulation governs the disclosure of CUI identified in DODD 5230.25, which applies to all unclassified technical information with military or space application (see glossary) in the possession of, or under the control of, a DOD component and information that may not be exported lawfully without approval, authorization, or license under the Export Administration Act (EAA) or Arms Export Control Act (AECA).

(3) *Channels of Official Foreign Disclosure Communications.*

(a) On behalf of the Secretary of the Army and the Chief of Staff, Army (CSA), the Deputy Under Secretary of the Army (International Affairs) (DUSA(IA)), Headquarters, DA (HQDA) or designee, is the exclusive DA point of contact (POC) for foreign military attachés diplomatically accredited to the United States (U.S.) Government (USG) and other representatives of foreign governments wishing to conduct official business with DA. However, the Deputy Chief of Staff for Intelligence (DCSINT), is the Army Executive Agent for all official foreign government requests for visits to DA commands or activities in the continental United States (CONUS) and U.S. Army information. All official foreign contacts with the Army in CONUS must be requested by diplomatically accredited military attachés on behalf of their respective governments.

(b) Except as authorized by the DUSA(IA) or senior Army leadership (Secretary of the Army, Under Secretary of the Army, CSA, Vice Chief of Staff, Army (VCSA) or Director of the Army Staff (DAS)), foreign representatives are not authorized official contact or communications with either DA personnel or DA organizations in any manner regarding any aspect of official business without prior authorization. Foreign representatives initiating such contact are to be informed that appropriate prior authorization for contact must be obtained on their behalf from the Office of the Deputy Chief of Staff for Intelligence (ODCSINT), HQDA by their respective military attachés. Except as required by AR 381-12, no report to ODCSINT, HQDA of such unauthorized contact is necessary.

(c) All foreign national (see glossary) requests, regardless of the mode of transmittal (that is, correspondence, e-mail, etc.), will be referred to the supporting Public Affairs Office for appropriate action. Except as required by AR 381-12, no report to ODCSINT, HQDA of such unauthorized contact is necessary.

(4) *Contacts with foreign representatives.* This regulation governs activities and actions involving representatives of foreign governments and international organizations. Inherent in all contacts with foreign representatives is the exchange of information in various forms—oral, visual or documentary. Policies governing the disclosure of DOD and DA information outside the USG prescribe that disclosed information must be suitable for disclosure to the public or to foreign governments or international organizations in furtherance of a legitimate USG purpose. This AR presumes that all contacts by foreign representatives with other than public affairs elements of the Army are for the exchange of

official information and thus must be authorized government-to-government or commercial exchanges. These contacts include the following—

(a) *Visits*. Visits by foreign representatives to organizations, agencies, activities, installations, and facilities over which DA exercises administrative control or security cognizance. This category includes visits to commercial firms performing work under contract to DA. DA contractors must follow the requirements of the International Traffic in Arms Regulations (ITAR), National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and, where applicable, the Export Administration Regulation (EAR).

(b) *Foreign Liaison Officer (FLO)*. A foreign government military member or civilian employee, who is authorized by his or her government to act as an official representative of that government in its dealings with the U.S. Army in connection with programs, projects or agreements of mutual interest to the U.S. Army and the foreign government.

(c) *Foreign Exchange Personnel*. Military or civilian officials of a foreign defense establishment who are assigned to a U.S. DOD Component (such as the U.S. Army), according to the terms of an applicable international agreement, and who perform duties, prescribed by a position description, for the DOD Component.

(d) *Cooperative Program Personnel (CPP)*. Foreign government personnel, assigned to an international program office hosted by DA or a foreign government pursuant to the terms of a Cooperative Program International Agreement, who report to and take direction from a DA Program Manager (PM) (or PM equivalent) for the purpose of carrying out the international program or project.

(e) *Meetings, Conferences, and Symposia*. Attendance by foreign representatives at meetings, conferences, and symposia sponsored or hosted by DA. (See AR 380-5)

b. This regulation designates specific DA officials (hereafter referred to as “designated disclosure authorities”) to perform the tasks listed below.

(1) Determine disclosure of DA CMI to foreign representatives.

(2) Identify foreign representatives authorized to receive DA CMI.

(3) Prescribe channels and methods used to obtain disclosure determinations, and explain how to physically accomplish transmittal of information.

c. This regulation prescribes duties and responsibilities of personnel designated as foreign disclosure officers (FDOs), who are DA members, designated, in writing, to oversee and control coordination of specific disclosures of CMI.

d. This regulation prescribes duties and responsibilities of personnel designated, in writing, as Army contact officers for foreign representatives who are visiting, certified as liaison officers, or assigned as exchange or CPP to DA commands or agencies.

e. This regulation does not govern the foreign disclosure of certain types of information the dissemination of which is handled through other than Army foreign disclosure channels. The types of information not covered by this regulation are listed below.

(1) *Sensitive compartmented information*. Sensitive compartmented information (SCI), including data related to equipment, methods, or techniques involved in production of SCI. (See AR 380-28)

(2) *National intelligence*. National and interdepartmental intelligence produced within the National Foreign Intelligence Board structure. (See AR 381-1)

(3) *Counterintelligence*. Counterintelligence operational information. (See AR 381-20)

(4) *Nuclear information*. Nuclear-related information (RESTRICTED DATA or FORMERLY RESTRICTED DATA). (See AR 380-150)

(5) *Strategic information*. Strategic planning information and related guidance, as designated by the Joint Chiefs of Staff (JCS).

(6) *Communications security*. Equipment or information relating to communications security (COMSEC), such as cryptographic devices and systems. (See AR 380-40)

(7) *NATO information*. Information that is in North Atlantic Treaty Organization (NATO) channels as a result of previously-approved foreign disclosure and has NATO classification markings. NATO information held by DA agencies and commands may be disclosed to a representative of NATO or one of its member nations if the prospective recipient has a valid need-to-know and possesses a current NATO security clearance. (See AR 380-5 and AR 380-15)

(8) *Automated information systems information outside of the continental U.S. (OCONUS) environment*. Unclassified information which has been, is, or can be deemed suitable for disclosure to local nationals employed in overseas U.S. Army computer/communications facilities. (See AR 380-19)

(9) *Special access programs*. Information covered under special access programs. (See AR 380-381)

(10) *Controlled unclassified information (CUI)*. Unclassified information not covered under paragraph 1-4a(2) to which access or distribution limitations have been applied according to national laws, policies, and regulations of the USG. These types of information include but are not limited to: patent secrecy data, confidential medical records, inter- and intra-agency memoranda which are deliberative in nature, certain data compiled for law enforcement purposes, data obtained from a company on a confidential basis, employee personal data, privacy act information, internal rules and practices of a Government agency which, if released, would circumvent an agency policy and impede the agency in the

conduct of its mission. Foreign governments and international organizations do not routinely request access to these types of CUI under U.S. Army international cooperative programs. As such, this regulation is not intended to cover such disclosures. CUI disclosures of this nature will be according to governing regulations. Note. Should these regulations not adequately address the disclosure of these types of information outside the USG, FDOs may use this regulation as a guide to ensure proper coordination and decision-making.

(11) *CMI to U.S. permanent residents.* For U.S. permanent residents (see glossary for definition of U.S. person), access to CMI is governed by AR 380-5.

(12) *Privacy Act information.* Information withheld from public disclosure under the Privacy Act. (See AR 340-21)

(13) *Information in the public domain.* Unclassified information that has been, is, or can be deemed suitable for disclosure to the public at large (that is, web sites, etc.), according to DODDs 5230.24 and 5230.25, and AR 360-5. Foreign governments can purchase public domain information from the Government Printing Office (GPO), Washington, DC and from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22151.

(14) *Export of information governed by the Department of Commerce.* Scientific, educational, or other data that qualify for general license under Department of Commerce export control regulations. (See EAR)

(15) *Information exempt from the requirement of a munitions license.* Information that may be exported under one or more of the general exemptions contained in subsection 125.4 of ITAR.

(16) *Federal legislation prohibition.* Classified information, the disclosure of which is prohibited by Federal Legislation.

(17) *Proprietary information.* Information (for example, trade secrets), the rights to which are owned by private firms or citizens, and cannot be disclosed without the owners' express written consent or other legal authorization.

f. The visit request requirements of this regulation are not intended to cover the following—

(1) Training of foreign personnel under invitational travel orders (ITOs). (See AR 12-15)

(2) Reciprocal exchanges of units for training purposes. (See AR 12-15)

(3) Cross-border movements of U.S. and Canadian forces. (See AR 525-16)

(4) Foreign students under a foreign military sales (FMS) program or private individuals attending school at educational facilities under contract with the Army or any other Governmental component. (See AR 12-15)

(5) Visits conducted at contractor facilities that involve access only to unclassified information, provided such information is authorized for disclosure pursuant to the Department of State's ITAR or the Department of Commerce's EAR, the applicable Government contract does not require a Government-approved visit authorization, and the visit will have no direct impact on DOD activities or responsibilities at the facility.

(6) Visits by foreign nationals, who are not representing their governments in an official capacity, to U.S. Army activities and DA contractor facilities.

(7) Unclassified visits by Canadian government officials and certified Canadian contractors under the U.S.-Canada Joint Certification Program (JCP) (See ITAR).

(8) Visits for activities that are open to the public.

(9) Visits that do not involve access to classified information or programs that are sponsored, controlled, administered, or recorded by the U.S. European Command under its Joint Contact Team Program, established according to Title 10, U.S. Code, Section 168, provided that the visitors are traveling on ITOs. This regulation also does not apply to visits by foreign representatives under ITOs from countries in the areas of responsibility of the other unified commands.

(10) Visits by foreign nationals participating in the U.S. Information Agency orientation tours (OTs).

g. This regulation specifically prohibits the disclosure under the following conditions:

(1) Information acquired from a foreign government or international organization to a third party without the written consent of the originator.

(2) Combined information (see glossary) without the consent of all parties that contributed to the product.

(3) Joint information (see glossary) without prior agreement of all parties having jurisdiction.

(4) Information originated by an agency outside of DA without the consent of the originator.

(5) The terms of a bilateral or multilateral agreement without the consent of all parties.

h. This regulation does not affect or modify the responsibility vested in the Director of Central Intelligence (DCI) pursuant to the National Security Act of 1947, as amended, and section 6 of the Central Intelligence Agency (CIA) Act of 1949, as amended, for protecting intelligence sources and methods from unauthorized disclosure. Further, any authority or responsibility vested in the Secretaries of State, Defense, or Energy, or the DCI is not affected by this regulation. Such authority and responsibility to make determinations regarding disclosures of classified information to foreign recipients are established by law, executive order, or other presidential authorization.

i. ODCSINT, HQDA encourages all commands and agencies to submit any request for exceptions or waivers to the policies and procedures of this regulation, with rationale, to this office (see appendix C, para C-2).

Section II Responsibilities

1–5. Deputy Under Secretary of the Army (International Affairs), HQDA

The DUSA(IA) will—

- a.* Exercise management oversight of Army functional policy regarding authorities for foreign disclosure, technology transfer, and munitions case processing.
- b.* Assess implications of proposed transfers of critical U.S. military technology.
- c.* Verify that proposed disclosures/transfers of critical U.S. military technology are consistent with national policy.
- d.* Coordinate and disseminate Army policy positions on munitions export license requests for both Munitions List and dual-use system technologies.
- e.* Ensure that all technology transfer criteria (see fig 2-1) are considered for each program for which the DUSA(IA) has primary responsibility (that is, security assistance, cooperative research and development (R&D), etc.).
- f.* Determine whether the proposed disclosure/transfer is consistent with previous export license application decisions and FMS cases.
- g.* Determine whether adequate technical and contractual safeguards have been devised to preclude the inadvertent diversion of critical U.S. military technology.
- h.* Initiate requests for ENDP in support of international programs.
- i.* Formulate, coordinate, establish, and disseminate weapon systems export policies, which will include intelligence threat assessments regarding regional impact of potential sales.
- j.* Review and coordinate Technology Assessment and Control Plans (TA/CPs) (see chap 4 and appendix D), Delegation of Disclosure Authority Letter (DDLs) (see appendix E), and other documents that affect the sale/transfer of equipment and information through FMS or direct commercial sales (DCS).
- k.* Provide political-military assessments and recommendations on the potential transfer of critical U.S. military technology.
- l.* Provide a representative to the Technology Control Panel (TCP).
- m.* Provide an Army member to represent the Secretary of the Army to the DOD Arms Transfer Policy Review Group.
- n.* Oversee the U.S. Engineers and Scientists Exchange Program (ESEP) (DOD term; Army term is Scientists and Engineers Exchange Program (SEEP)).
- o.* Oversee the Standardization Representative (StanRep) (see glossary) Program.
- p.* Serve as Army proponent for all U.S.-sponsored foreign dignitary visits and OTs.
- q.* Administer, manage, and execute the U.S. Army CPP Program.
- r.* Oversee Latin America (LATAM) Cooperation activities.
- s.* Chair the Technology Transfer Security Assistance Review Panel (TTSARP).

1–6. Deputy Chief of Staff for Intelligence (DCSINT), Headquarters, Department of the Army (HQDA)

The DCSINT, HQDA will—

- a.* Subject to the direction of DUSA(IA), formulate Army policies governing contact with and disclosure of CMI to foreign representatives and provide general guidance, advice, and assistance to DA officials determining the suitability of CMI and CUI identified for foreign disclosure. Such action will be according to the National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations, short title: National Disclosure Policy (NDP-1), DODD 5230.11, and DODD 5230.20, DODD 2040.2, and DODD 5530.3. The DCSINT will—
 - (1) Exercise exclusive approval authority for disclosure of DA CMI to foreign representatives.
 - (2) Exercise authority to delegate disclosure of CMI to DA subordinate elements (major Army Commands (MACOMs) and below), as well as delegate authority to specific DA subordinate elements to approve certain types of visits by foreign representatives.
- b.* Provide an Army member to represent the Secretary of the Army to the National Disclosure Policy Committee (NDPC).
- c.* Control internal distribution of NDP-1 and provide necessary delegated disclosure authority to implement NDPC Records of Action (RAs) (see glossary) throughout DA.
- d.* Subject to the direction of DUSA(IA), formulate Army policies governing the international technology transfer program and be the primary POC for technology transfer security issues within HQDA (see chap 4). In this role, the DCSINT will—
 - (1) Task appropriate HQDA elements to prepare technical assessments, as needed, identify militarily critical technologies, and provide additional technical support for international technology transfer issues.
 - (2) Task specific agencies to conduct intelligence, counterintelligence, and operations security (OPSEC) assessments, as appropriate, of information, technologies and systems proposed for disclosure or transfer.

- (3) Provide staff review of all Army actions with technology transfer implications.
- (4) Ensure that appropriate protection measures are considered for each program that potentially involves the international transfer of CMI.
- (5) Provide representation to the TTSARP.
- (6) Chair the TCP (see chap 4).
- e.* Ensure that disclosure decisions involving CMI are recorded in the Foreign Disclosure Technical Information System (FORDTIS), in compliance with DOD Instruction (DODI) 5230.18.
- f.* Record decisions on foreign visits to DA elements in the Foreign Visits System (FVS), in compliance with DODI 5230.18.
- g.* Exercise authority over the Foreign Liaison Officer (FLO) Program.
- h.* Coordinate, review and submit all Army Exceptions to NDP-1 (ENDPs) (see appendix C) requests.
- i.* Conduct oversight over the foreign disclosure training program.
- j.* Exercise exclusive authority over the approval of all Army Delegation of Disclosure Authority Letters (DDLs).
- k.* Assist in the review of munitions license applications referred to HQDA for an Army recommendation, according to the criteria set forth in AR 12-8 and NDP-1.

1-7. Heads of HQDA Staff Agencies and MACOM Commanders

Heads of HQDA staff agencies and MACOM Commanders will—

- a.* Ensure that their personnel follow the provisions of this regulation and any additional guidance, when interacting with foreign representatives.
- b.* Designate a POC for each HQDA staff agency. Designate, in writing, a single official to be the FDO for each MACOM.
- c.* Exercise and delegate, as needed, disclosure authority for CUI that is originated under the provisions of their regulations.
- d.* Publish agency or MACOM guidance that will —
 - (1) Ensure that all CMI being considered for foreign disclosure is referred to the FDO for appropriate coordination. The final foreign disclosure decision will be in compliance with NDP-1.
 - (2) Ensure disclosure decisions involving CMI are recorded in FORDTIS.
- e.* Provide support to the Army international technology transfer program, as appropriate.
- f.* Report and process violations of policies and procedures contained in this regulation in the manner prescribed for compromise of CMI, as provided in AR 380-5, chapter 6. A copy of all such reports will be provided to ODCSINT, HQDA.
- g.* Appoint contact officers (see glossary), in writing, for all official foreign visitors to all echelons of their command or agency.
- h.* Ensure PMs oversee the transfer of classified technologies and weapon systems through direct commercial sales (DCS) for compliance with established Army disclosure and export policies.
- i.* Conduct periodic on-site visits to organizations, agencies, activities, installations, and facilities over which MACOMs exercise administrative control or security cognizance, to ensure compliance with this regulation.
- j.* Formulate, establish, coordinate, and disseminate policy and procedures for the disclosure of CUI under their purview. Note: Commands and agencies may elect to use the policy and procedures for the disclosure of CMI outlined in this regulation as a guide.

1-8. Deputy Chief of Staff for Operations and Plans (DCSOPS), HQDA

The DCSOPS, HQDA will—

- a.* Assess operational impact on U.S. forces if a U.S. Army weapon system were to be illegally transferred to a U.S. adversary.
- b.* Assess to what extent a proposed weapons system transfer will have on U.S. military engagement and operational plans, and to what degree the system or item counters that country's military threat.
- c.* Ensure that the disclosure criteria cited in chapter 2 of this regulation are considered for each international program for which the Deputy Chief of Staff for Operations (DCSOPS) has primary responsibility, and which potentially involves the international transfer of CMI.
- d.* Assess implications of proposed disclosures/transfers on DCSOPS programs, plans, and policies.
- e.* Provide a representative to the TCP and TTSARP.
- f.* Administer, manage, and execute the U.S. Military Personnel Exchange Program (MPEP) (DOD term; U.S. Army term is Personnel Exchange Program (PEP)).
- g.* Formulate, establish, and disseminate operations security and physical security policy and procedures regarding access, badging, escorts, and vehicle decal identification of foreign visitors.

1-9. Assistant Secretary of the Army (Acquisition, Logistics and Technology (ASA(ALT)))

The ASA(ALT) will—

- a.* Identify critical U.S. military system-specific technologies.
- b.* Task preparation of and validate TA/CPs and Summaries of Statement of Intent (SSOIs) (See appendix F).
- c.* Assist in review of munitions export licenses referred to HQDA for policy determination, according to the criteria set forth in AR 12-8.
- d.* Provide technical experts on DA, DOD, and interagency committees, panels, and working groups that address technology transfer and militarily critical technologies.
- e.* Identify critical applied and emerging military technologies.
- f.* Provide direct staff support to the Army member of the DOD Arms Transfer Working Group.
- g.* Ensure technology transfer security is considered for each Army program that potentially involves the international transfer of CMI.
- h.* With the DUSA(IA) and The Judge Advocate General (TJAG), devise effective technical and contractual safeguards to prevent the inadvertent diversion of critical U.S. technology.
- i.* Have HQDA responsibility for formally coordinating the DOD Militarily Critical Technologies List (MCTL).
- j.* Provide a representative to the TCP and TTSARP.
- k.* Ensure foreign disclosure guidance on materiel items is provided to HQ, U.S. Army Training and Doctrine Command (TRADOC) FDO, in sufficient detail to support Program of Instruction development.
- l.* Ensure program executive office (PEO) PMs coordinate with their Army Materiel Command (AMC) matrix security support regarding all classified issues dealing with foreign disclosure and international technology transfer according to AR 70-1.
- m.* Ensure PEO PMs oversee the transfer of classified technologies and weapon systems through DCS for compliance with established Army disclosure and export policies.

1-10. Deputy Under Secretary of the Army (Operations Research) (DUSA(OR)), HQDA.

The DUSA(OR) will—

- a.* Serve as the DA proponent for modeling and simulation.
- b.* Identify and disseminate information regarding critical technologies in modeling and simulation that should not be transferred to foreign entities.

1-11. Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM)

CG, INSCOM will—

- a.* Provide counterintelligence and security support to Army activities involved in international technology transfer and foreign disclosure matters.
- b.* Provide a representative as an observer to the TCP.
- c.* Provide tailored, multi-disciplined counterintelligence threat briefings on technologies (subject to potential foreign technology transfer) to DA agencies and commands hosting foreign visitors. Debrief those Army personnel having contact with foreign visitors, when appropriate.
- d.* Conduct counterintelligence investigations into spying, unauthorized removal and retention of CMI, and known or suspected unauthorized disclosure of CMI, to include military technology, and research and development data on acquisition systems.

1-12. Commanding General, U.S. Army Materiel Command (CG, AMC)

CG, AMC is responsible, according to Army policy guidelines provided by HQDA for the execution of the Army's Technology Transfer (see glossary) Program. CG, AMC may delegate authority to accomplish the spirit and purpose of international technology transfer control. Specifically, the CG, AMC will—

- a.* Designate a single POC for technology transfer in HQ, AMC.
- b.* Develop assessments to identify militarily critical and emerging technologies required for development, production, or operation of U.S. Army systems, and identify and provide an assessment of relative risks and benefits of international cooperation and the transfer of those technologies.
- c.* At ASA(ALT) direction, provide technical representatives and assistance to support DA and interagency working groups, committees, and panels on international technology transfer and militarily critical technologies.
- d.* As directed by and in coordination with DCSOPS, HQDA, assess whether effective technical and contractual safeguards can be devised to preclude the inadvertent diversion of critical military technology in conjunction with any proposed transfer.
- e.* At ASA(ALT) direction, provide technical experts to participate in Wassenaar Arrangement (multinational export control regime) list reviews, as required, and ensure that the opinions rendered by those experts accurately reflect the Army position on any given technology.

- f. Provide technical guidelines, recommendations, assistance, and data regarding control of technology transfer to foreign countries.
- g. As directed by DCSOPS, HQDA, provide continuing assessment of technology transfer control mechanisms and their effectiveness.
- h. Coordinate intelligence assessments for all proposed international cooperative programs.
- i. Ensure foreign disclosure guidance on materiel items is provided to HQ, TRADOC FDO, in sufficient detail as to support Program of Instruction development.
- j. Provide a representative to the TCP.
- k. Ensure PMs oversee the transfer of classified technologies and weapon systems through DCS for compliance with established Army disclosure and export policies.

1–13. The Judge Advocate General

TJAG will—

- a. Together with DUSA(IA) and ASA(ALT), determine whether adequate technical and contractual safeguards can be developed to preclude the inadvertent diversion of critical technology.
- b. Provide a legal advisor to the Chairman of the TCP.
- c. Provide direct staff support to the Army member of the DOD Arms Transfer Working Group and the NDPC.
- d. Review, prior to the initiation of negotiations for legal sufficiency, all proposals regarding the establishment of international agreements.

1–14. The Surgeon General (TSG), the Chief of Engineers (COE), and the Director, Information Systems for Command, Control, Communications and Computers (DISC4)

TSG, COE, and DISC4 will—

- a. Ensure that technology transfer factors and implications are considered for each international program for which they have primary responsibility and which potentially involves the disclosure of CMI.
- b. Provide a representative to the TCP.
- c. For DISC4: Formulate, establish, and disseminate policy and procedures for access to computers and computer networks, to include foreign representatives and nationals.

1–15. CG, U.S. Army Criminal Investigation Command (USACIDC)

CG, USACIDC is responsible for investigating felony criminal cases that involve international technology transfer issues. CG, USACIDC will—

- a. Investigate export violations, as detailed in 50 USC § 2410 and 50 USC § 2411.
- b. Provide copies of final reports to the DCSINT, HQDA of investigations regarding the illegal disclosure of CMI.
- c. Serve as POC to coordinate with the U.S. Customs Service and Department of State regarding the enforcement of international technology transfer laws or regulations.
- d. If required, provide a representative as an observer to the TCP.

1–16. Overseas major commanders

Overseas major commanders are to use the policy guidance contained in this regulation to establish local policies and procedures governing interactions with foreign representatives. For this purpose, overseas major commanders are U.S. Army Europe; U.S. Army Pacific; U.S. Army Southern Command; and Eighth U.S. Army. Army overseas major command components of unified commands are to adhere to unified command policies and procedures insofar as such policies and procedures are consistent with applicable DA guidance. ODCSINT, HQDA will be advised of any conflict between unified commands and DA guidance. Significant conflicts will be resolved at the DA/DOD level.

1–17. Other Overseas Army Activities

Other overseas Army activities assigned to or under operational control of overseas major commands will adhere to the overseas major commands' policies and procedures governing interaction with foreign representatives.

Chapter 2

General Disclosure Policies, Authority to Disclose, and Delegation of Authority

Section I

Introduction

2–1. Concept

- a. *National Security Strategy summary.* The goal of the President's National Security Strategy (NSS) is to ensure the

protection of our nation's fundamental and enduring needs: protect the lives and safety of Americans, maintain the sovereignty of the U.S. with its values, institutions and territory intact, and promote the prosperity and well-being of the nation and its people. The NSS and its companion document, the National Military Strategy (NMS), stress that "the imperative of engagement" is vital to our security. Because America is engaged worldwide, even in peacetime, significant portions of our Armed Forces are present overseas or readily available to deploy overseas, where many of our interests are found. This posture of global engagement, combined with peacetime military engagement, which encompasses all U.S. military activities involving other nations, help shape the security environment. Engagement serves to demonstrate our commitment; improve interoperability; reassure allies, friends and coalition partners; promote transparency; convey democratic ideals; deter aggression; and help relieve sources of instability before they can become military crises.

b. Role of Foreign Disclosure in U.S. National Security Strategy. U.S. sharing of its military resources (that is, CMI resident in technology, materiel, etc.) is a critical component of our engagement. CMI is a national security asset or resource. It may be disclosed to foreign governments and international organizations only under certain conditions: First, the national security and other legitimate interests of the USG must be demonstrably furthered by doing so. Second, the information must be approved for disclosure by the appropriate USG disclosure official. Third, the country must be eligible for the information to be disclosed and the disclosure criteria and conditions of NDP-1, as set forth in this chapter, must be satisfied. The proper application of the provisions of NDP-1 will facilitate the timely disclosure of CMI and transfer of critical technologies and materiel to allied and friendly non-allied countries, and, at the same time, will afford the proper protection of these critical military technologies and materiel, thereby contributing significantly to the attainment of U.S. NSS and NMS (engagement) goals and objectives.

c. CMI Disclosure Support to National Security Strategy. While U.S. participation in bilateral or multilateral agreements does not automatically authorize the disclosure of CMI to their participants, the lack of an international agreement does not necessarily preclude disclosure. Each potential disclosure of CMI must be evaluated on its own merit. A disclosure determination must be made by a designated disclosure authority, following the criteria established in this regulation.

2-2. False Impression

U.S. policy is to avoid creating false impressions of its readiness to make available classified military materiel, technology, or information. Therefore, initial discussions with foreign governments and international organizations concerning programs which might involve the eventual disclosure of CMI may be conducted only if it is explicitly understood and acknowledged that no U.S. commitment to furnish such classified information or material is intended or implied until disclosure has been approved. Accordingly, proposals to foreign governments and international organizations which result from either U.S. or combined initial planning and which may lead to the eventual disclosure of classified military materiel, technology, or information, including intelligence threat data or countermeasures information, must be authorized by designated disclosure officials in the departments and agencies originating the information, or by the NDPC.

2-3. Categorization of Military Information

a. CMI. CMI is information that a competent authority has determined to be of such sensitivity that it requires special designation and protection in the interest of national security, that it must be subject to special controls, and that access to it must be limited to personnel whose successful performance of duty clearly requires such access (need-to-know) and who have been specifically cleared for such access. According to its degree of sensitivity, CMI is identified by levels of security classification: CONFIDENTIAL, SECRET, or TOP SECRET. (See AR 380-5 for details regarding the classification of defense information.)

b. Unclassified information. Information that a competent authority has determined not to require the degree of protection afforded by the application of a security classification. (See paragraph 1-4 of this regulation for additional information.)

(1) *CUI.* Certain unclassified information may be of such sensitivity as to warrant placing a degree of control over its use and dissemination—to further various national interests—whereas other unclassified information may not warrant any control over its dissemination. For the purpose of this regulation, the former kind of unclassified information is termed CUI.

(2) *Public Domain.* For the purposes of this regulation, unclassified information that does not qualify for the status of CUI—as described in b(1) above—is deemed to be actually or potentially in the public domain; that is, suitable for disclosure to the public at large. In all cases, all U.S. Army information must be reviewed prior to release to the public. The proponent for the disclosure of U.S. Army public domain information is the U.S. Army Public Affairs Office.

2-4. Categories of Military Information

a. To facilitate the decision process for foreign disclosure, the NDP-1 divides CMI into eight categories. Designations and definitions of these categories are described below.

b. Unclassified information is not formally categorized, but the designations and descriptions below may be used and are encouraged for use as a baseline for decision making.

(1) *Category 1 (Organization, Training and Employment of Military Forces)*. Military information of a general nature necessary to the organization of military, paramilitary, or irregular forces, to include those tactics, techniques, and tactical doctrine (including intelligence and counterintelligence) necessary to train and employ those forces. This category does not include specific technical data and training necessary to operate and maintain individual items of military materiel and munitions.

(2) *Category 2 (Military Materiel and Munitions)*. All military materiel, arms and munitions procured and controlled by the USG for the equipping, operation, maintenance and support of its military forces or the military, paramilitary, or irregular forces of its allies. Items developed by U.S. private interests as a result of USG contracts or derived from technology paid for by the USG are included within this category. This category also comprises information to include technical data and training necessary to operate, maintain, or support specific military materiel, arms, or munitions.

(a) *Build-to-print*. Assumes the country receiving the information has the capability to replicate an item, sub-system or component from technical drawings and specifications alone without technical assistance. Disclosure of supporting documentation (for example, acceptance criteria, object code software for numerical controlled machines) is permissible. Disclosure of any information which discloses design methodology, engineering analysis, detailed process information or manufacturing know-how associated with the end-item, its subsystems or components is excluded. Build-to-Print is not considered production information and will be handled through normal Category 2 technology transfer channels.

(b) *Assembly information*. Normally associated with hardware (parts or kits to be assembled, special tooling or test equipment to accomplish specific tasks) and information which allows assembly and testing of the finished product. Only top level drawing will be disclosed. Detailed assistance is not to be provided, wherein such assistance would provide production or manufacturing techniques. Assembly Information is not considered production information and will be handled through normal Category 2 technology transfer channels.

(3) *Category 3 (Applied Research and Development Information and Materiel)*. Military information resulting from the extension of fundamental theories, designs, and data from purely theoretical or experimental investigation into possible military applications to include research, the construction and testing of prototypes and such design changes affecting qualitative performance as may be required during the service life of an item. This also includes engineering data, general operational requirements, concepts and military characteristics required to adopt an item for production. Development ceases when materiel has completed operational suitability testing or has for all practical purposes been adopted for military use or production. It includes tactics, techniques and tactical doctrine pertaining to specific equipment not yet in production or yet approved for adoption by U.S. forces.

(4) *Category 4 (Production Information)*:

(a) *Manufacturing Information*. This includes the know-how, techniques and processes required to produce or substantially upgrade military materiel and munitions. A manufacturing process or technique is a set of instructions for transforming natural substances into useful materials (metals, plastics, combustibles, etc.) or fabricating materials into aerodynamic, mechanical, electronic, hydraulic, or pneumatic systems, subsystems, and components. Software source code including related documentation that describes software or development know-how for a particular U.S. warfare system which has completed Acquisition Milestone II or documentation used for production thereof are considered to be design and manufacturing data and equivalent to Category 4 (Production Information). A manufacturing data package describes how to manufacture, test and accept the item being produced and what tools are required. Types of manufacturing information include drawings, process sheets, wiring diagrams, instructions, test procedures and other supporting documentation. Software source code and software documentation that contain or allows access/insight to classified algorithms or design rationale are considered to be manufacturing information. Unclassified software source code and software documentation that is required for minor software maintenance, interface/integration, or to make administrative changes to tables, symbols, markers, displays will be handled through normal Category 2 technology transfer channels.

(b) *Build-to-print and assembly information*. See paragraph 2-4b(2)(a) and (b) of this chapter.

(5) *Category 5 (Combined Military Operations, Planning and Readiness)*. That information necessary to plan, assure readiness for and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. Includes installations located within the territory under jurisdiction of, or of direct concern to, the recipient foreign government or international organization.

(6) *Category 6 (U.S. Order of Battle)*. Information pertaining to U.S. forces located within territory that is under the jurisdiction of a recipient government or is otherwise of direct concern to a foreign government or an international organization. In general, authorization for disclosure is limited to U.S. Order of Battle in the recipient countries or in adjacent geographical areas.

(7) *Category 7 (North American Defense)*. North American Defense (NORAD) information concerning plans, programs, projects, operations, and certain specific technical data pertaining to equipment directly related to NORAD, particularly when it is originated by or under the control of NORAD. It includes—

- (a) Plans and related documents prepared by combined U.S./Canada defense agencies;
- (b) U.S. operational and logistics plans for employment of reserve forces; and

(c) Information revealing the vulnerability of a NORAD area, or vulnerability or official appraisal of combat readiness of any unit or facility, or the effectiveness of NORAD systems.

(8) *Category 8 (Military Intelligence)*. Military Intelligence comprises information of a military character pertaining to foreign nations and is subject to the criteria for disclosure of intelligence stated in the NDP-1.

2-5. Maximum Delegated Disclosure Levels

The NDPC has established maximum classification levels within each category of CMI that may be disclosed to foreign governments or international organizations by DA. Maximum classification levels are depicted on charts in Annex A of NDP-1, which is accessible through FORDTIS.

a. To exercise the disclosure authority delegated to DA, CMI under consideration for foreign disclosure must not exceed the established maximum classification level for the nature of the information in question as outlined in NDP-1.

b. CMI exceeding the maximum classification level may still be considered for disclosure if significant U.S. interests warrant it. Basic disclosure criteria, conditions, and limitations in paragraphs 2-6 and 2-7 below must be fully satisfied. The HQDA staff agency or MACOM proposing or supporting disclosure of the CMI in question may propose an ENDP.

c. ENDPs, other than those specifically granted by the Secretary of Defense or Deputy Secretary of Defense, will be granted only by the NDPC. All Army requests for ENDPs will be forwarded through command or agency channels to the appropriate HQDA proponent for coordination and submission to ODCSINT, HQDA, which reviews, coordinates, and submits the request to the NDPC. (See appendix C and figs C-1 and C-2.)

2-6. Basic Disclosure Criteria

All decisions for disclosure of CMI are judged on a case-by-case basis.

a. Categories 1-7. Disclosures in Categories 1 through 7 may be made when all of the following criteria are addressed and satisfied—

(1) Political and Military Criteria. Disclosure is consistent with U.S. foreign policy, national security objectives, and military security objectives regarding the recipient foreign government or international organization (see fig 2-1).

(2) Security Assurances.

(a) *Disclosure is contingent upon security assurances provided by a foreign government.* The Departments of State and Defense have concluded General Security of Military Information Agreements (GSOMIAs) and other bilateral security arrangements with various foreign governments. These security agreements or arrangements outline the responsibilities of both parties pertaining to the safeguarding of U.S. CMI. The existence of a security agreement or arrangement with a foreign government satisfies the security assurance requirement for that foreign government. In exceptional circumstances, fulfillment of U.S. interests may require disclosure of CMI to foreign elements without a formal agreement providing for adequate security protection. A disclosure of this nature may be authorized by ODCSINT, HQDA, after appropriate coordination with national agencies having a direct interest in the disclosure. If authorized, the foreign recipient will meet the following conditions:

1. The information or acknowledgment of its possession will not be revealed to a third party, except with the prior consent of the U.S. originating department or agency.

2. The information will be used for specified military-related purposes only.

3. The recipient will report promptly and fully to U.S. authorities any known or suspected compromise of U.S. CMI disclosed to them.

4. All individuals and facilities that will have access to CMI will have security clearances granted by their government at a level equal to that of the classified information involved and an official need-to-know.

5. The foreign recipient of the information has agreed to abide by or meet U.S.-specified special terms and conditions for the disclosure.

(b) *The foreign recipient has the capability and willingness to afford it substantially the same degree of security protection given to it by the USG.* Guidance in determining a foreign government's capability and willingness to protect U.S. information may be determined by a U.S. embassy security assessment, CIA risk assessment, or NDPC security survey report.

(3) *U.S. Benefits.* Disclosures will result in benefits to the U.S. at least equivalent to the value of the information disclosed. For example:

(a) The U.S. obtains information from the recipient nation on a quid-pro-quo basis.

(b) The exchange of military information or participation in a cooperative project will be advantageous to the U.S. from a technical or other military standpoint.

(c) The development or maintenance of a high level of military strength and effectiveness on the part of the foreign government receiving the information will be advantageous to the USG.

(4) *Disclosure Limits.* The disclosure is limited to information necessary to the purpose for which disclosure is made.

b. *Category 8.* Disclosures in Category 8 (Military Intelligence) will be made according to NDP-1.

Political considerations:

- a. The potential foreign recipient's support for U.S. foreign policy and political objectives.
- b. The potential of the transfer to deny or reduce an influence or presence in the country that is hostile to U.S. interests.
- c. The effects of the regional and global strategic balance if the transfer is approved.
- d. Whether or not the country has a defense treaty or political agreement with the U.S.
- e. The political benefits that could accrue to the U.S.
- f. Whether or not the transfer assists the U.S. in obtaining or securing base, transit, and overflight rights or access to strategic locations.
- g. Other countries to which the U.S. has transferred the item.
- h. The possible reaction of other countries in the region to the proposed sale.
- i. Whether or not the U.S. is the first supplier of the item.
- j. The possibility that the item could fall into the hands of terrorists.
- k. The impact of the transfer on the country's economy.
- l. Whether or not the transfer establishes an unfavorable political precedent.

Military considerations:

- a. The degree of participation in collective security by the U.S.
- b. How the transfer would affect coalition warfare in support of U.S. policy.
- c. How the item would increase the recipient country's offensive or defense capability.
- d. How the transfer would increase the capability of friendly regional forces to provide regional security to assist the U.S. in the protection of strategic line of communication.
- e. How the transfer will strengthen U.S. or allied power projection.
- f. To what extent the transfer is in consonance with U.S. military plans.
- g. Whether or not the export is consistent with Army regional RSI policy.
- h. Whether or not the system or item is a force structure requirement.
- i. Can the country's technology base support the item?
- j. To what degree the system or item counters the country's threat.
- k. To what extent the system constitutes part of an appropriate force and systems mix.

Figure 2-1. Political and military criteria

-
- l. Logistical (maintenance, parts, instruction, personnel, changes, or updates) support that will be required.
 - m. What components are classified? What elements are really critical? Does the system or do its components represent a significant advance in the state-of-the-art?
 - n. What precedent exists for disclosure of this particular technology or system? Are comparable systems (foreign or domestic) using the same technology already in the marketplace?
 - o. Can the critical technology resident in the system be reverse engineered? If so, what level of effort (in terms of time, funding and manpower) is required based on the technological capability of the foreign recipient?
 - p. Has the technology or information resident in one U.S. Army weapons program been leveraged from another U.S. Army weapons program? If so, has the original U.S. Army weapons PM reviewed and rendered a recommendation on the munitions license request? The technology or information may not be listed as CPI for one program, but identified as CPI for another program.
 - q. Are there any special considerations involved with the disclosure that requires coordination external to the U.S. Army? For example, COMSEC, low observable, cryptologic information, etc. If so, has proper approvals been obtained?

Figure 2-1. Political and military criteria—Continued

2-7. Establishment of disclosure programs pursuant to international agreements

- a. The disclosure of DA CMI to foreign governments or international organizations may be prompted by DA participation in activities stemming from international and functional agreements negotiated and concluded according to applicable ARs. Upon conclusion, these agreements form the basis on which disclosure determinations will be made.
- b. DA must avoid giving the false impression that the DA may subsequently approve classified disclosures. DA officials responsible for reviewing, providing input, or negotiating an agreement must ensure that the CMI disclosure implications of potential agreements are identified prior to the initiation of discussions regarding such agreements.
- c. A proposed or draft agreement is to be examined in its entirety to determine whether any aspect of it might result in the disclosure of CMI. Examination must not be limited to introductory or promotional material, but must consider possible follow-on disclosures of CMI that could result from the disclosures initially proposed. Initial examination occurs at the appropriate command or agency at which the proposed agreement originates. It will be accomplished with the technical assistance of the command or agency FDO to ensure the agreement complies with the policies prescribed in this regulation. DA proponents will ensure that the views of all affected parties (including the U.S. Defense Attaché Office (USDAO), etc.) are obtained and considered (if appropriate) for incorporation into the draft agreement.
 - (1) If the FDO determines that only unclassified information will be disclosed, the FDO will provide a disclosure recommendation regarding whether non-binding preliminary discussions will commence.
 - (2) If the FDO determines that CMI will or is likely to be disclosed, the FDO will provide a disclosure recommendation regarding whether non-binding preliminary discussions should commence. If the decision is to commence non-binding preliminary discussions, the FDO will –
 - (a) Ensure that the discussions are marked with a caveat, stipulating that any disclosure is not to be construed as a USG commitment to engage in any cooperative venture.
 - (b) Refer one-time (see section II, para 2-9m of this chap) CMI disclosure requests to the appropriate HQDA proponent for consideration. The HQDA proponent will complete coordination as may be necessary among other HQDA agencies before requesting disclosure authority from ODCSINT, HQDA.

Section II

Authority to Disclose CMI and CUI and Delegation of Disclosure Authority

2-8. CUI disclosure authority and delegation of authority

HQDA agency heads and MACOM commanders are delegated the authority to disclose CUI covered by this regulation. This delegation of authority may be further delegated to the lowest echelon that may be an originator or proponent of CUI. In making disclosure decisions on CUI covered by this regulation, the originator or proponent will use the disclosure criteria cited in section I of this chapter. In all cases, the disclosure of CUI to foreign representatives requires the consent of the originator or proponent. Note: Since the foreign disclosure community has traditionally been the central point of contact for the majority of official foreign government requests, all official government requests involving CUI will continue to be processed administratively through the appropriate FDO for staffing and ensuring the proper closure of cases.

2-9. CMI disclosure authority and delegation of authority

Under the provisions of NDP-1, the responsibility for decisions to disclose CMI is delegated to the Secretary of the Army. On behalf of the Secretary of the Army, the DCSINT, HQDA exercises exclusive authority to render decisions on the disclosure of CMI originated by or for DA for which DA is the DOD component having primary substantive interest or which is otherwise determined to be under the security and disclosure cognizance of DA by this regulation. ODCSINT, HQDA delegates CMI disclosure authority to certain HQDA officials, as listed below. These HQDA officials are delegated disclosure authorities and will approve or deny the disclosure of CMI, but this delegation of disclosure authority applies only to CMI in which the HQDA official the original classification authority and is limited to the categories and eligibility levels cited in NDP-1. For CMI for which the HQDA official is not the original classification authority, disclosure will be according to NDP-1 and requires the written approval of the original classification authority. Disclosure authorization from these designated HQDA officials are always required.

a. Category 1. Officials listed in the subparagraphs below have the authority to make disclosure determinations for Category 1 CMI (Organization, Training, and Employment of Military Forces). This authority applies within the substantive scope of agreements that provide for rationalization, standardization, and interoperability (RSI) and have been approved according to AR 34-1, AR 550-51, or both.

- (1) DCSOPS, HQDA.
- (2) DISC4, HQDA.
- (3) DUSA(IA), HQDA.
- (4) TSG.

b. Category 2. Officials listed in the subparagraphs below have authority to make disclosure determinations regarding Category 2 CMI (Military Materiel and Munitions). This authority applies to information requested in furtherance of security assistance-related sales, grants, leases, or loans or reciprocal use of items for which a positive determination of U.S. willingness to sell or transfer has been rendered under AR 12-1 and AR 12-8. Also included are items adopted for allied or friendly RSI.

- (1) DUSA(IA), HQDA.
- (2) ASA(ALT).
- (3) TSG.
- (4) DCSOPS, HQDA.
- (5) DISC4, HQDA.
- (6) Deputy Chief of Staff for Logistics (DCSLOG), HQDA.

c. Category 3. Officials listed in the subparagraphs below have authority to make disclosure determinations for Category 3 CMI (Applied Research and Development Information and Materiel). This authority applies within the substantive scope of international cooperative R&D agreements approved under AR 70-33, AR 70-41, and AR 550-51, and pertains to information about developmental materiel items approved for allied and friendly government RSI or in furtherance of security assistance-related sales for which a positive determination of U.S. willingness to sell or transfer has been rendered under AR 12-1 and AR 12-8.

- (1) OASA(ALT).
- (2) DCSOPS, HQDA.
- (3) DISC4, HQDA.

d. Category 4. Disclosures of Category 4 CMI (Production Information) must be approved by ODCSINT, HQDA on a case-by-case basis.

e. Category 5. The following officials have authority to make disclosure determinations concerning Category 5 CMI (Combined Military Operations, Planning and Readiness). This authority applies within the substantive scope of international agreements approved under AR 550-51 and regarding allied or friendly government RSI.

- (1) DCSOPS, HQDA.
- (2) TSG.

f. *Category 6.* The following officials have authority to make disclosure determinations for Category 6 CMI (U.S. Order of Battle):

- (1) DCSOPS, HQDA.
- (2) Deputy Chief of Staff for Personnel (DCSPER), HQDA.
- (3) DCSLOG, HQDA.

g. *Category 7.* Disclosure determinations for Category 7 CMI (NORAD) will be accomplished according to NDP-1.

h. *Category 8.* Disclosure determinations for Category 8 CMI (Military Intelligence) will be accomplished according to NDP-1.

i. HQDA agency heads will ensure that all disclosures of CMI by their respective agencies are reported to ODCSINT, HQDA for recording into FORDTIS.

j. ODCSINT, HQDA will issue DDLs to selected MACOMs through command channels, as well as to selected MSCs with the concurrence of the respective MACOM.

k. *Re-delegation.* Re-delegation of the disclosure authority is not authorized without specific written authorization (that is, DDL) from ODCSINT, HQDA, which exercises exclusive authority over the issuance of DDLs. Fully justified proposals regarding further delegation of disclosure authority will be submitted through command or agency channels to ODCSINT, HQDA. If approval is granted, ODCSINT, HQDA will issue a DDL.

l. *Emergency authority.* Under conditions of actual or imminent hostilities, MACOM Commanders are delegated disclosure authority to disclose CMI up to and including the SECRET level to an actively participating allied force when support of combined combat operations requires the information, and the eligibility and criteria requirements established in NDP-1 are satisfied. ODCSINT, HQDA, in cooperation with the Office of the Joint Chiefs of Staff (OJCS) and the MACOM, will determine, as soon as practicable, the limitations that should be imposed on continuing disclosures of such information. MACOMs will notify the ODCSINT, HQDA of such disclosures at the earliest possible date.

m. *One-time CMI disclosure requests.* One-time CMI disclosures include command initiatives to provide CMI to a foreign government or international organization, as well as Army responses to foreign-initiated visit or information requests in those cases where no disclosure authorization exists.

(1) *Authority.* ODCSINT, HQDA is the sole approval authority for proposed one-time CMI disclosures.

(2) *Procedures.* Commands or agencies must submit one-time CMI disclosure requests, in writing, to the appropriate HQDA proponent designated in section II, paragraph 2-9 of this chapter. If the appropriate HQDA proponent concurs in the proposal, the request will be forwarded to the ODCSINT, HQDA for disclosure determination. Requests should arrive at ODCSINT, HQDA at least 5 working days prior to the planned disclosure and must include the following information:

(a) Description of information proposed for disclosure in sufficient detail that adjudication can be made. This information must include the category involved, identification of the proponent of each item proposed for disclosure, and a position from that proponent with respect to the disclosure to the requesting foreign government.

(b) Rationale for the disclosure.

(c) Benefit to the Army/USG.

(d) Disclosure restrictions.

ODCSINT, HQDA will notify the appropriate command or agency of its decision.

2-10. Delegation of Disclosure Authority Letter

A DDL is a document issued by ODCSINT, HQDA explaining classification levels, categories, scope, and limitations of information under Army's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate commands and agencies. A DDL will be prepared collectively by the host DA command or agency proponent for the international activity involved, FDO, and subject matter expert, and forwarded through command or agency channels to ODCSINT, HQDA for approval. If the DDL is part of a more comprehensive proposal, the DDL will be forwarded as part of the entire packet to the HQDA proponent. For example, a proposal involving the establishment of a new FLO position for assignment to a PEO PM will be forwarded through PEO channels to OASA(ALT) for appropriate staffing. ODCSINT, HQDA is the approval authority for all DDLs and revisions to DDLs. Local FDOs may approve changes to the contact officer. DDLs are intended for internal Army use only and will not be provided to or its contents disclosed to foreign representatives (see appendix E).

2-11. Responsibilities and establishment of foreign disclosure officers

A FDO is a DA member designated, in writing, to oversee and control coordination of specific disclosures of CMI. FDOs are authorized for appointment to the lowest command or agency level that is the proponent for Army-originated, developed, or derived CMI. *Note: The FDO will be responsible for the administrative processing of all requests for CUI. The disclosure decision for CUI will be the proponent or originator that effected the control of that information.*

a. *FDO Appointments.* FDO appointments will be in writing. Notification of such appointments will be made to MACOMs, which will provide ODCSINT, HQDA a consolidated FDO list annually.

b. FDO Training. All FDOs are required to attend the Foreign Disclosure Training Course sponsored by ODCSINT, HQDA. Funds for travel, per diem, and overtime, if required, will be provided by the ODCSINT, HQDA (as funds are available). All FDOs will attend the Foreign Disclosure Training Course within 2 calendar years from the date of this regulation. The DCSINT, HQDA encourages all non-FDO personnel that interact with foreign representatives or deal with international programs, to attend this course. Attendance will be on a space-available basis. Funding will be the responsibility of sponsoring command or agency. Appendix G provides a reference list of frequently asked questions regarding foreign disclosure that all FDOs should be able to answer.

2–12. Foreign disclosure channels and general decision procedures

To promote prompt and judicious disclosure determinations, while maintaining the required degree of control and providing operational flexibility, it is essential to establish specific channels in which to process foreign disclosure requests.

a. ODCSINT, HQDA role. ODCSINT, HQDA is to receive and respond to all foreign disclosure requests for CMI. In the situations cited below, ODCSINT, HQDA has issued DDLs or equivalent disclosure guidance to the appropriate commands or agencies to receive and respond to foreign disclosure requests.

- (1) A request by a foreign representative during an approved visit is to be addressed by the designated DA host.
- (2) A request by a certified FLO, foreign exchange officer, or CPP is to be addressed directly to the DA agency or command to which the individual is certified. That agency or command will render a response.
- (3) A request by a certified British, Canadian, or Australian Armies StanRep is to be addressed directly to the DA command or agency to which the StanRep is certified. The command or agency will render a direct response in the case of information on projects listed on the American, British, Canadian, and Australian (ABCA) Armies Standardization List and determined to be releasable under the provisions of this regulation. Requests for information for which the command or agency is not the sole proponent will be fully coordinated with all affected commands or agencies. Denials will be referred to the ABCA U.S. National Standardization Officer (NSO) within the Office of the DUSA(IA) (ODUSA(IA)), HQDA for resolution.
- (4) Requests relating to the acquisition of defense articles and services or relating to munitions licenses are to be processed through security assistance channels to ODUSA(IA).
- (5) Requests rendered in channels specified in certain approved international cooperative R&D agreements (that is, Defense Development Exchange Program (DDEP) agreements according to AR 70-33, etc.) are to be addressed by the proponent of the international agreement.
- (6) Requests addressed to OCONUS MACOM components of unified commands in channels specified in certain international agreements providing for combined planning and operations are processed by the Army Component Command.
- (7) Requests through Defense Technical Information Center (DTIC) are sent to the FDO of the command or agency originating the document. Recommended denials of CMI regarding documents from DTIC will be referred to ODCSINT, HQDA for resolution.

b. Foreign disclosure requests.

- (1) All requests for the disclosure of CMI to a foreign government or international organization, irrespective of point of receipt within DA, will be referred through command channels to the HQDA staff agency or MACOM exercising applicable program responsibility, unless disclosure authority has been delegated.
- (2) The only exception is the PEO system. After coordinating and obtaining a position from its major subordinate command (MSC) matrix support FDO, PMs under the cognizance of a PEO may elect to refer their foreign disclosure requests directly to ASA(ALT), HQDA. In the event of a major difference of positions between a PM under the PEO system and his or her MSC matrix support, the PM may refer the request to ASA(ALT), HQDA along with the dissenting MSC matrix support position. ASA(ALT) will coordinate the action within HQDA prior to rendering a decision under a DDL (if applicable) or submitting the action to ODCSINT, HQDA for a disclosure decision.

c. Coordination and development of disclosure recommendations/decisions.

- (1) Prior to rendering a decision on the recommendations or forwarding the recommendations to HQDA for a decision, if required, MACOMs and MSCs will coordinate with all affected DA agencies to develop a fully staffed and coordinated MACOM or DA agency position.
- (2) Comments and recommendations on issues related to the disclosure of CMI will address to what degree the disclosure request satisfies each of the basic disclosure criteria cited in this chapter. Additionally, the following considerations should assist commands or agencies in formulating recommendations:
 - (a) Whether the information has previously been approved for disclosure to another foreign government of substantially equivalent status and, if so, when, by whom, and in what form or context.
 - (b) Whether the foreign government in question possesses the capability and expertise to use and protect the information effectively.
 - (c) Whether approval of the disclosure in question would affect current or projected DA activities.
 - (d) Whether the information being considered for disclosure includes or concerns any of the types of information

cited in paragraphs 1-4e(1) through 1-4e(9). If so, the comments must clearly state the type of information and identify which portions of the information being considered for disclosure are involved.

(e) Whether the information falls within the substantive scope of an existing international agreement, which the recipient government has signed. If it does, the following must be identified: NATO panel or working group designator; ABCA Armies Standardization Program; working group or party, or appearance on standardization list; data exchange agreement or annex (DEA); or, memorandum of agreement (MOA) or other agreement by title and date.

(f) Whether similar information at a lower classification level would satisfy the disclosure requirement being considered. If so, identify the benefits to the U.S. Army of disclosing information classified at a higher level.

(g) Whether the issue requires substantive coordination with other DA agencies. If so, documentation reflecting such coordination must be attached.

(h) Whether the issue has been identified at the Army senior leadership level as having special interest for or against international participation. For example, has the Army Acquisition Executive identified the issue as one requiring special coordination action at HQDA, over and above the normal review process?

(i) Whether the issue requires coordination outside DA (such as, with the Office of the Secretary of Defense (OSD), other Military Service components, industrial proprietary concerns or other countries).

Chapter 3

Modes, Methods, and Channels for CMI Disclosures and Related Administrative Procedures

Section I

Procedures for Disclosure to or by Visitor, Exchange, Cooperative, and Liaison Personnel

3-1. Concept

a. In no instance will DA CMI be disclosed or transmitted to other than the authorized representatives of the foreign government(s) or international organization(s) for which disclosure has been approved.

b. Disclosure of DA CMI will sometimes occur as a result of—

(1) Visits by—

(a) Foreign representatives to organizational elements or facilities under the jurisdiction or security cognizance of DA. These facilities include U.S. companies performing work under contract to DA. Visits include attendance at or participation in meetings, conferences, and symposia sponsored or co-sponsored by DA elements. (See appendices H through J for further details.)

(a) DA representatives to organizational elements or facilities under the jurisdiction or security cognizance of foreign governments or international organizations.

(2) Certification of—

(a) FLOs and StanReps certified to DA (see appendices K and L).

(b) U.S. Army liaison officers and StanReps to foreign governments and international organizations.

(c) Foreign representatives assigned to the DA work force (see appendices M through O).

(d) DA representatives assigned to the work forces of foreign governments and international organizations.

(3) Other foreign requests and DA-initiated proposals to disclose information in documentary form.

(4) Requests initiated by U.S. agencies—other than DA—for DA-originated CMI.

3-2. DA CMI Disclosed During Visits

Disclosure of CMI in conjunction with an official visit is contingent on approval of disclosure to the foreign government or international organization involved. Such disclosure determinations will be made by DA officials designated as disclosure authorities. CMI disclosures must be limited to that information authorized to be disclosed to accomplish the purpose of the visit. What is considered essential will be viewed from a U.S. perspective only.

a. Foreign visits to DA activities and DA contractors in CONUS.

(1) *Official visits.* (See glossary for definition of visit authorizations). Official visits to DA elements and DA contractors by foreign representatives, irrespective of the source of the initiative or funding, will be according to appendix J of this regulation.

(2) *Administrative requirements.*

(a) For visits conducted under the International Visits Program, a visitor's foreign government-issued security clearance status and the required security assurance will be conveyed through official foreign Requests for Visit Authorization (RVAs).

(b) For other visits, the DA sponsor is responsible for obtaining and disseminating clearances, as well as security assurances, as applicable. These will be communicated to prospective DA hosts. Such data may be acquired from a CONUS-based foreign military attaché office or the appropriate USDAO.

(3) *Modes of disclosure.* CMI disclosures to foreign visitors by DA or DA contractors will normally be in an oral or visual mode, or both. At the discretion of the FDO, an exception to allow the disclosure in documentary form (to include notes taken during briefings or discussions) may be made, provided that the visit request security assurance specifically states that the individual may assume custody on behalf of the foreign government and ODCSINT, HQDA approves the request. The DA host agency or command will transmit such notes in the manner prescribed for document disclosures in section III of this chapter. A receipt must be obtained for classified material provided to foreign representatives, regardless of its classification level.

(4) *Discussions beyond approved visit purpose.* Visitor requests for discussions outside the approved purpose will be denied, with a recommendation to direct the request to the foreign military attaché for action.

b. Official DA visits to establishments of foreign governments and international organizations. DA personnel traveling OCONUS under AR 55-46, if such travel involves official interaction with foreign representatives, may be authorized to disclose DA CMI, if such disclosure is mission essential. The fact that and extent to which such authorization has been granted are to be reflected in area clearance-related communications prescribed in AR 55-46.

3-3. DA CMI disclosed to or by FLO, Foreign Exchange, and Cooperative Program personnel

See paragraph 3-2 above and appendices J through O for detailed information.

3-4. Documentary requests for U.S. CMI

Most disclosures of DA CMI occur through the direct personal interaction described in the preceding paragraphs of this section. However, certain types of foreign government requests are not prompted by personal interaction. These types of requests, which must be submitted in writing, are for disclosures of DA CMI in documentary form. They are submitted to ODCSINT, HQDA, unless ODCSINT, HQDA has specifically authorized other channels to be used (as noted in para 2-12). The subparagraphs below provide guidelines for processing document requests.

a. *Security Assistance.* Foreign requests for CMI documents regarding the provision of defense articles and services (including publications) will be submitted or referred to AMC/U.S. Army Security Assistance Command (USASAC), through established security assistance channels. On receipt, AMC/USASAC will—

(1) Verify that the requester's authority to procure defense articles and services under a security assistance program is legitimate.

(2) Coordinate with all affected DA parties and approve, deny, or refer the request to DUSA(IA) for actions involving disclosure authority above that delegated to the command or agency. This action will be pursuant to AR 12-8 and the policies prescribed in this regulation.

(3) Respond on behalf of DA to the authorized foreign representative of the customer country.

b. *R&D.* Approved international cooperative R&D agreements with accompanying DDLs normally designate specific channels for responding to requests for R&D documents. If so, requests must be submitted through those channels. On receipt of requests, DA authorities designated in an R&D agreement are to—

(1) Verify that the requester's involvement in the agreement is authentic and that the request is within the scope of the agreement.

(2) Accomplish necessary coordination among other affected parties within DA.

(3) Approve or deny the disclosure according to delegated authority or refer the matter to the echelon exercising disclosure authority.

(4) Respond on behalf of DA. The approved materials will be provided to the applicable CONUS-based foreign military attaché (or designee), USDAO or U.S. Security Assistance Office (SAO).

c. *Defense Technical Information Center Document Requests.* The 11 July 1990 Memorandum of Understanding (MOU) signed by the Departments of Army, Air Force, and Navy, DIA, and DTIC, established standard procedures for disclosure determinations regarding DTIC AD-numbered document requests by the governments of Australia, Canada, and the United Kingdom. Since that time, additional foreign governments have been granted DTIC accounts. Foreign government requests will be processed as follows—

(1) DTIC will send foreign government requests for CMI or CUI (for administrative processing) to the FDO of the command or agency that originated the document.

(2) The FDO will coordinate the request with the originator or proponent.

(3) The command or agency will effect further coordination, as required.

(4) If disclosure approval is recommended, originator or proponent will sanitize (as required) and forward the CMI or CUI document, and DTIC Form 55 (Defense Technical Information Center Request for Release of Limited Document) through the FDO to the requesting embassy and DTIC, respectively.

(5) If denial is recommended for a CMI document, the command or agency will forward the document and DTIC Form 55, with justification for denial, to ODCSINT, HQDA for final disclosure determination and closure of the case. If the originator or proponent denies the disclosure of the CUI document, the command or agency will forward the document and DTIC Form 55 to DTIC, thereby closing the case.

d. *Other Categories.* Foreign requests for documentary information regarding matters other than in the preceding subparagraphs will be initiated by the embassies according to table 3-1 and the accompanying notes. When the

instructions contained in table 3-1 stipulate the request will be sent to ODCSINT, HQDA, these requests, if validated, will be processed in the following manner:

- (1) Logged in and assigned a case number.
- (2) Coordinated with external organizations, as required.
- (3) Staffed to the command or agency having cognizance over the information.
- (4) The recipient of the staffing is to obtain a copy of the document, review and complete Army coordination with all affected DA commands or agencies, as required.
- (5) For proprietary data requests, forward the request to the owner of the proprietary data for action and provide a copy of the letter to the requesting embassy. The FDO will notify ODCSINT, HQDA of the action taken to close the case.
- (6) If the fulfillment of the request only requires the disclosure of CUI, the originator or proponent will—
 - (a) If approved, mark the document and forward it through the FDO to the requesting embassy, according to section III of this chapter.
 - (b) If denied, collaborate with the FDO on the preparation and transmittal of a letter to the embassy.
 - (c) FDO will notify ODCSINT, HQDA of the disclosure decision.
 - (d) ODCSINT, HQDA will administratively close the case.
- (7) If the fulfillment of the request requires the disclosure of CMI, the commander or agency head (if delegated disclosure authority) will—
 - (a) If approving under an ODCSINT, HQDA-issued DDL or approval granted by another delegated disclosure authority, mark and sanitize the document, as required, and forward the document to the requesting embassy as prescribed in section III of this chapter. The FDO will notify ODCSINT, HQDA of the final decision.
 - (b) If it is not covered by an existing DDL, forward the document to ODCSINT, HQDA for action. Provide a recommendation and detailed justification.
 - (c) ODCSINT, HQDA will administratively close the case.

Section II

Foreign Access to Automation

3-5. Foreign access to computers and computer networks.

FLOs, foreign representatives assigned to the MPEP, ESEP, and CPP programs, and official foreign government visitors may not have unsupervised access to computer systems (stand-alone or network), unless the information accessible by the computer is authorized for disclosure to their government and the appropriate accreditation authority has granted access according to AR 380-19. Disclosures of CMI to these foreign representatives will be according to the provisions of this regulation. If a foreign representative is given access to a computer network, the local area network administrator must place a caveat or marker (spell out the country name of foreign representative, do not use acronym) on all outgoing e-mails identifying that person as a foreign representative. This procedure will ensure that the recipient of the e-mails, both internal and external to the foreign representative's organization, is aware of the sender's status as a foreign representative. Note: In the case of foreign national employees of the USG working under a DA contract or agreement, access to information resident in computers or computer system networks will be limited to that unclassified data required to fulfill the terms of the contract or agreement. AR 380-19, paragraph 2.17, provides guidance regarding these individuals.

3-6. Secret Internet Protocol Router Network (SIPRNET).

SIPRNET is a Secret, System High, U.S.-only common user network encompassing Intelink-S, Global Command and Control System, and Joint Worldwide Intelligence Communications System.

a. SIPRNET terminals must remain under strict U.S. control at all times. This applies to terminals that are directly or indirectly connected to the SIPRNET. When SIPRNET terminals are located in workspaces physically accessible to foreign representatives (such as combined operations centers), SIPRNET terminals must be grouped together in an U.S.-controlled terminal space.

b. If a foreign representative is authorized access to the U.S.-controlled terminal space, he or she must be announced, screens must be covered or blanked, the visitor must wear a badge clearly identifying them as a foreign representative, and he or she must be escorted at all times. If the foreign representative is permitted to view the screen, U.S. personnel must ensure that no classified information beyond that stated in the foreign representative's DDL is visible on the screen. The foreign representative will not be permitted to control the terminal in any way. As an additional precaution, screen savers with password protection must be used on all SIPRNET terminals in combined workspaces, as described above. If a foreign representative working at an U.S. Army site has a requirement for access to a local area network with either a direct or indirect connection to the SIPRNET, the U.S. Army commander at that site must submit a foreign access request, through command channels, to DISC4, HQDA.

3-7. Non-Secure Internet Protocol Routing Network (NIPRNET).

DOD's unclassified, but sensitive, U.S.-only common user routed data network is used primarily for information purposes. Access is granted to DOD personnel with .mil extensions. If a foreign representative is given access to NIPRNET, the assigned e-mail address will comply with the conditions cited in paragraph 3-5.

Section III Administrative Procedures

3-8. Concept

Before DA CMI approved for foreign disclosure is actually transferred in documentary form, certain actions are required to avoid false impressions and proliferation of requests for CMI that clearly are not to be disclosed to the requestor. Responsibility for sanitizing information that is not to be disclosed to the requestor lies with the originator or proponent. The originator or proponent will certify to the FDO that the publication has been sanitized to the extent necessary. The DA command or agency approving disclosure will adhere to the following guidelines:

- a.* Delete references to documents and information that are not to be disclosed to the foreign requestor.
- b.* Provide only the information that satisfies the requestor's specific requirements.
- c.* Prohibit the disclosure of documentary information in draft form.
- d.* Prohibit the disclosure of foreign government CMI or proprietary information without approval, in writing, from the foreign government or contractor in question.
- e.* Remove or obliterate all distribution lists and bibliographic data (bibliographies, lists of references, bibliographic notes).

3-9. Physically conveying CMI documentary material

a. CMI in documentary form is generally conveyed to recipient foreign governments either by hand or by mail. If conveyed by mail, the material is to be addressed to the appropriate CONUS-based foreign military attaché or USDAO. In addition—

- (1) CMI conveyed by hand or by mail is to be packaged and handled as prescribed in AR 380-5, chapter 8.
 - (2) For all CMI, regardless of method of conveyance, the disclosing DA command or agency will use DA Form 3964 (Classified Document Accountability Record) to record the dispatch of the CMI and obtain acknowledgement of its receipt. Receipts are to be retained as prescribed in AR 25-400-2 and AR 380-5.
- b.* CMI to be conveyed in documentary form to NATO commands or agencies are to be introduced into NATO channels according to AR 380-5, AR 380-15, and AR 25-51.
- c.* CMI to be conveyed in documentary form to international partners in multinational cooperative projects that is not appropriate for all members of the project will be processed in compliance with the procedures of this section, but be annotated on the front and back covers: (U.S. classification), releasable to (list applicable countries) ONLY.

3-10. Recording CMI disclosure determinations and transfers

Foreign Disclosure and Technical Information System (FORDTIS) is an important database that records the first-time disclosures of U.S. CMI to foreign government and international organizations. The purpose of FORDTIS is to assist DA decision-makers and analysts in reviewing, coordinating, and rendering decisions or recommendations regarding proposals requiring the disclosure of CMI to foreign governments and international organizations. By recording these entries, FORDTIS can provide a tracking mechanism of the foreign disclosure of all U.S. Army CMI. It can also serve as a retrieval tool that can be used to present a comprehensive picture of the disclosures of U.S. Army CMI to a foreign government or international organization regarding a specific international program, such as a cooperative R&D project or a security assistance case. Additionally, by capturing all first-time foreign disclosures of U.S. CMI, FORDTIS can reduce the disclosure decision processing time. For example, if FORDTIS indicates that the CMI being requested for disclosure to a specific foreign government or international organization has been previously disclosed to that foreign government, the disclosure decision process ends and the command or agency receiving the request approve the disclosure of the requested CMI. Therefore, if FORDTIS is to fulfill its purpose, the expeditious entry of all first-time disclosures of U.S. CMI is a critical administrative responsibility for all echelons of the U.S. Army.

- a.* All adjudications regarding foreign disclosure of CMI will be recorded in FORDTIS by the appropriate command or agency.
- b.* FORDTIS is designed to record decisions regarding foreign disclosure of CMI. These include munitions licenses, strategic trade issues, Exception to National Disclosure Policy (ENDPs), visits by foreign representatives, certification of foreign representatives, and miscellaneous disclosure determinations (that is, all cases not related to the other five types). The DA command or agency that makes the disclosure determination is responsible for recording the data within 20 working days of the actual disclosure.

c. DA agencies or commands having FORDTIS terminals will record data on-line. Those not having an on-line capability will complete DD Form 1822 (Report of Disclosure or Denial of U.S. Classified Military Information) (RCS: DD-POL (AR) 1661). DD Form 1822 will be forwarded through command foreign disclosure channels to the first level of command or technical supervision having an on-line capability. Specific instructions governing both FORDTIS on-line entries and the completion of DD Form 1822 are contained in DOD 5230.18-M.

Table 3-1
Document Request Procedures

Item	If Information Desired is	And the Requester	And Information is	Then the Requester Must
1	Available through GPO or NTIS. (See Note 1)	(N/A)	(N/A)	Acquire the information directly from the GPO or NTIS.
2	Contained in a DA administrative publication (e.g., Army regulation, pamphlet, circular, field/technical manual, AR-TEP, etc.)	a. Maintains a publications account with USASAC. (See Notes 2 and 5)	(1) UNCLASSIFIED	Acquire the information directly from USASAC.
			(2) CLASSIFIED	Submit written request to USASAC.
		b. Is not eligible to obtain a publications account with USASAC.	(N/A)	Submit written request to ODCSINT, HQDA.
3	Technical information regarding the purchase, maintenance, or production of equipment/materiel; or secondary item supply status on accepted sales cases. (See Note 3)	a. Is certified to HQ, AMC.	(1) UNCLASSIFIED	Acquire the information from USASAC. (See Note 4)
			(2) CLASSIFIED	Submit written request to USASAC.
		b. Is certified to HQ, AMC.	(N/A)	Submit written request to USASAC.
4	Contained in U.S. Army Service School publications (e.g., programs of instruction, lesson plans, special texts, study pamphlets, reference data, and other instructional material.)	(Same as Item 3)	(Same as Item 3)	(Same as Item 3)
5	In the form of training films or training aids.	(Same as Item 3)	(Same as Item 3)	(Same as Item 3)
6	Maps.	(N/A)	(N/A)	Acquire the information from the Defense Intelligence Agency, ATTN: COS-4, Washington, DC 20301
7	Contained in Military or Federal Standardization Documents (e.g., specifications, standards, handbooks, and lists of qualified industries.)	(N/A)	(N/A)	Acquire the information directly from the Standardization Document Order Desk, Bldg 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.
8	Contained in professional magazines and journals (e.g., Army Magazine, Infantry Magazine, Armor Magazine, etc.).	(N/A)	(N/A)	Acquire the information directly from the publisher.
9	Under the auspices of a legally-approved Data or Information Exchange Annexes (DEA/IEA).	(N/A)	(N/A)	May acquire the information only via the appropriate Technical Project Officer (TPO) or Associate TPO (ATPO).

**Table 3-1
Document Request Procedures—Continued**

Item	If Information Desired is	And the Requester	And Information is	Then the Requester Must
10	Other than those cited in Items 1-9.		(N/A)	Submit written request to ODCSIINT, HQDA.

Notes:

¹ Addresses for GPO and NTIS are:

Superintendent of Documents
Government Printing Office
710 North Capital Street, NW
Washington, DC 20402

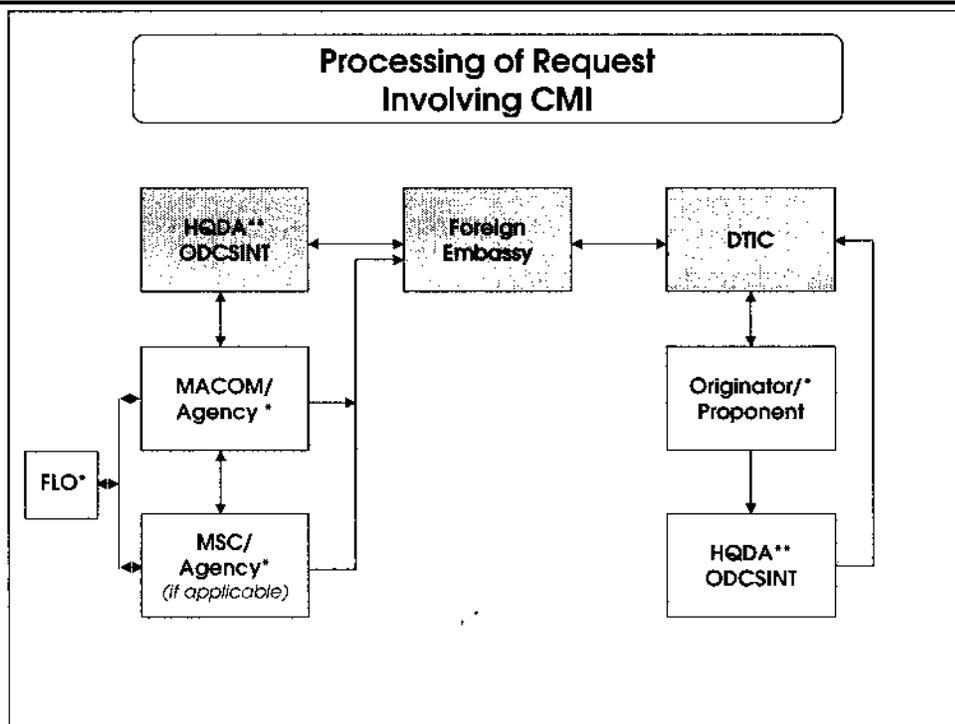
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

² Countries which are eligible to enter into FMS arrangements with the U.S. Army may be eligible to establish an FMS publications account with the U.S. Army Publishing Agency for the purpose of obtaining Army administrative publications. Military Attachés representing potentially eligible countries should inquire on the eligibility of their respective parent governments. For those eligible, the Army expects that such accounts will be established and maintained. The Chief of Foreign Liaison will not provide administrative publication accounts with The U.S. Army Publishing Agency.

³ Other types of communications which are directly related to the actual or proposed acquisition of U.S. Army equipment and material under the auspices of FMS, may also be referred directly to the Commander, U.S. Army Security Assistance Command, ATTN: DRSAC-SC, 5001 Eisenhower Avenue, Alexandria, VA 22333.

⁴ Requests for documentary information which are to be submitted directly to USASAC, are to be prepared in accordance with the format and instructions depicted in the Policies and Procedures Manual provided to all embassies by HQDA.

⁵ Requests originated by authorized foreign representatives of the customer country in the U.S. should be sent directly to USASAC or its designees.



NOTES

- * Permitted to approve request provided CMI is within the scope of its DDL and classified by its original classification authority or previously disclosed to the requesting foreign government. If CMI is not originally classified by the command or agency receiving the request, lateral coordination must be accomplished with the original classification authority. If authorized, FLOs may submit requests involving CMI to host commands or agencies.
- ** If request for CMI is not within DDLs of any MSCs and MACOMs, the request shall be forwarded to ODCSINT, HQDA for disclosure determination.

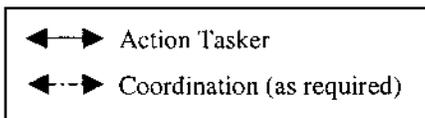


Figure 3-1. Processing of request involving CMI

Chapter 4 International Technology Transfer Program

4-1. Concept

This chapter describes the significance and the attention devoted to the Army international technology transfer program. The senior Army leadership recognizes the significance of international technology transfer in attaining our NSS and NMS goals and objectives, and has established the Technology Control Panel (TCP) to review and develop policy for the U.S. Army relating to its critical technologies. Additionally, the acquisition community also recognizes this importance and has instituted the requirement for all PMs to develop technology protection documents in support of their respective programs. The establishment of the TCP and the institution of technology protection documents clearly illustrate the senior Army leadership's commitment to balancing the sharing of its critical technologies with the requirements to protect those same critical technologies.

4-2. Technology Control Panel

a. Purpose of the TCP.

(1) The DCSINT, HQDA has established the TCP as a coordinating mechanism to assist in carrying out the responsibility to manage and coordinate international technology transfer issues for the Army.

(2) The TCP is intended to facilitate rational and consistent non-routine international technology transfer decisions based on comprehensive consideration of relevant factors.

b. Function of the TCP. The TCP will—

(1) Develop and recommend Army international technology transfer control policy to the DCSINT on a case-by-case basis.

(2) Ensure quality of control of Army international technology transfer actions.

(3) Consider contentious or priority issues on a case-by-case basis, as deemed necessary by the TCP chairperson.

c. TCP Composition.

(1) The TCP will consist of the following members:

(a) A representative of DCSINT-Chairperson.

(b) A representative of DUSA(IA).

(c) A representative of ASA(ALT).

(d) A representative of DCSOPS.

(e) A representative of DISC4.

(f) A representative of TSG.

(g) A representative of TJAG.

(h) A representative of TRADOC.

(i) A representative of Forces Command (FORSCOM).

(j) A representative of Space and Missile Defense Command (SMDC).

(k) A representative of AMC.

(2) The TCP will consist of the following observers:

(a) A representative of INSCOM.

(b) A representative of USASAC.

(c) A representative of USACIDC.

d. TCP Chairperson, Member, and Observer Responsibilities.

(1) Each TCP member and observer will designate an alternate.

(2) Representatives and observers from other Army elements and MACOMs may be invited by the Chairperson to participate, as needed.

(3) The Chairperson will designate an executive secretary from the ODCSINT, HQDA, who will be responsible for all administrative support, including space, equipment, and clerical support. Funds for travel, per diem, and overtime, if required, will be provided by the parent organization of each TCP member or observer.

(4) The TCP will meet quarterly or as required as determined by the TCP Chairperson.

4-3. International technology transfer documentation

The following international technology transfer documents are essential parts of the Army's Technology Protection Program:

a. Technology Assessment/Control Plan. The TA/CP is a DOD-mandated technology protection document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the impact of international transfer of the resulting system; and the development of measures to protect the U.S.

technological or operational advantage represented by the system. It is required for all major defense acquisition programs and international agreements, particularly when the disclosure of CMI is envisioned. Development of the TA/CP is the responsibility of the PM, in concert with appropriate international cooperative program offices and foreign disclosure/security offices. In acquisition programs, the TA/CP is a required annex to the Program Protection Plan (PPP) and must be completed no later than Milestone 1. Format for a TA/CP is found at appendix D. Attached to each TA/CP for classified defense acquisition programs and international agreements is a DDL, which describes the scope and limitations about information, to include training, that may be disclosed to specific foreign governments. The formats used for DDLs are at appendix E.

b. Summary Statement of Intent. The SSOI is a DOD-mandated international cooperative programs document. It is required for all international R&D cooperative programs and replaces the TA/CP requirement for those programs. Development of SSOI is the responsibility of the materiel developer, in concert with the appropriate international cooperative program offices and foreign disclosure/security offices. Format for a SSOI is found at appendix F. A DDL is required for all international R&D cooperative programs involving CMI and is forwarded as a companion document to the SSOI.

c. Program Protection Plan. The PPP is another DOD-mandated document required for acquisition programs. Development of PPP is the responsibility of the materiel developer, in concert with the appropriate international cooperative program offices and foreign disclosure/security offices. The purpose of the PPP is to identify critical program information (CPI), technology and systems (formerly, essential program information, technology and systems or EPITS) to be protected and to create a management plan that outlines measures to be taken by the PM necessary to protect the weapon system throughout the acquisition process. CPI is defined as information, technologies, or systems that, if compromised, will degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. CPI should be identified at Milestone 0, or as soon as possible thereafter, within the acquisition lifecycle. The PPP should be completed no later than Milestone 1. DODD 5200.39 and DOD 5200.1-M implement the PPP.

Appendix A References

Section I Required Publications

AR 34-1

International Military Rationalization, Standardization and Interoperability. (Cited in paras 2-9a, H-3, and I-8b(1).)

AR 55-46

Travel Overseas. (Cited in para 3-2b.)

AR 70-58

International Professional Scientists and Engineers Exchange Program. (Cited in paras I-8c and N-1.)

AR 380-5

Department of the Army Information Security Program. (Cited in paras 1-4a(1), 1-4a(4)(e), 1-4e(7), 1-4e(11), 3-9a(1), 3-9a(2), 3-9b, and H-5c.)

AR 550-51

International Agreements. (Cited in paras 2-9a, 2-9c, 2-9e, D-1a, I-9a, M-1, and O-3a.)

AR 614-10

US Army Personnel Exchange Program With Armies of Other Nations; Short Title: Personnel Exchange Program. (Cited in paras I-8c, M-1, and M-3.)

DODD 5230.11

Disclosure of Classified Military Information to Foreign Governments and International Organizations. (Cited in paras 1-6a and E-5.) (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5230.20

Visits, Assignments, and Exchange of Foreign Nationals. (Cited in paras 1-6a, E-5, J-6, and K-3a.) (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5230.25

Withholding of Unclassified Technical Data From Public Disclosure. (Cited in paras 1-4a(2) and 1-4e(13)). (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

Section II Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this publication.

AR 5-11

Management of Army Models and Simulations

AR 11-31

Army International Affairs Policy

AR 12-1

Security Assistance, International Logistics, Training, and Technical Assistance Support Policy and Responsibilities

AR 12-8

Security Assistance - Operations and Procedures

AR 12-15

Joint Security Assistance Training (JSAT) Regulation

AR 25-30

The Army Integrated Publishing and Printing Program

AR 25-51

Official Mail and Distribution Management

AR 25-55

The Department of the Army Freedom of Information Act Program

AR 25-400-2

The Modern Army Record Keeping System (MARKS)

AR 70-1

Army Acquisition Policy

AR 70-23

The Technical Cooperation Program (TTCP)

AR 70-26

Department of the Army Sponsorship of Unclassified Scientific or Technical Meetings

AR 70-31

Standards for Technical Reporting

AR 70-33

Mutual Weapons Development Data Exchange Program (MWDDEP) and Defense Development Exchange Program (DDEP)

AR 70-35

Research, Development, and Acquisition

AR 70-41

Cooperation With Allies and Other Nations in Research and Development of Defense Equipment

AR 70-45

Scientific and Technical Information Program

AR 70-57

Military-Civilian Technology Transfer

AR 70-66

United States-Canadian Defense Development Sharing Program

AR 95-1

Flight Regulations

AR 190-13

The Army Physical Security Program

AR 210-50

Housing Management

AR 340-21

The Army Privacy Program

AR 360-5

Army Public Affairs, Public Information

AR 380-15 (C)

Safeguarding Classified NATO Information (U). (Stocked and issued at the following address: ASNS-OPB, Room 1B889, Pentagon, Washington, DC 20310.)

AR 380-19

Information Systems Security

AR 380-28 (C)

The Department of the Army Special Security System (U)

AR 380-40 (O)

Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (U)

AR 380-67

Department of the Army Personnel Security Program

AR 380-150

Access to and Dissemination of Restricted Data

AR 380-381

Special Access Programs (SAPS) (U)

AR 381-1

Control of Dissemination of Intelligence Information

AR 381-12

Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 381-20

The Army Counterintelligence Program

AR 525-16

Temporary Cross-Border Movement of Land Forces Between the United States and Canada

530-1

Operations Security (OPSEC)

DODD 2000.9

International Co-Production Projects and Agreements Between the United States and Other Countries or International Organizations. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 2040.2

International Transfers of Technology, Goods, Services, and Munitions. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODI 3200.14

Principles and Operational Parameters of the DoD Scientific and Technical Information Program. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 4500.54

Official Temporary Duty Travel Abroad. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5000.1

Defense Acquisition. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODI 5000.2

Defense Acquisition Management Policies and Procedures. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5100.55

United States Security Authority for North Atlantic Treaty Organization Affairs. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DOD 5105.38-M

Security Assistance Management Manual. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DOD 5200.1-M

Acquisition Systems Protection Program. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DOD 5200.1-R

Information Security Program Regulation. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5200.12

Conduct of Classified Meetings. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5200.39

Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DOD 5220.22-M

National Industrial Security Program Operating Manual (NISPOM). (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODI C-5220.29

Implementation of the North Atlantic Treaty Organization Industrial Security Procedures (U). (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODI 5230.18

The DOD Foreign Disclosure and Technical Information System (FORDTIS). (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DOD 5230.18-M

Foreign Disclosure and Technical Information System (FORDTIS) User Manual. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5230.24

Distribution Statements on Technical Documents. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5400.7

DOD Freedom of Information Act Program. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

DODD 5530.3

International Agreements. (Available on the World Wide Web at the following address: <http://www.defenselink.mil>.)

ITAR

International Traffic in Arms Regulation. (Available on the World Wide Web at the following address: www.pmdtc.org.)

MCTL

Militarily Critical Technologies List (Available on the World Wide Web at the following address: www.dtic.mil/mtcl.)

NDP-1 (S)

National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations. (Provided to Designated Disclosure Authorities on a need-to-know basis by the ODCSINT, HQDA)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

DA Form 11-2-R

Management Control Evaluation Certification Statement

DA Form 3964

Classified Document Accountability Record

DA Form 4605-R

Department of the Army Munitions Control Case Processing Worksheet

DD Form 254

Department of Defense Contract Security Classification Specification

DD Form 1822

Report of Disclosure or Denial of U.S. Classified Military Information

DTIC Form 55

Defense Technical Information Center Request for Release of Limited Document

Appendix B

Management Control Evaluation Checklist and DA Staff Assistance and Compliance Visits

B-1. Function

This checklist covers the administration, supervision, and control of the foreign disclosure of CMI and contacts with foreign representatives.

B-2. Purpose

The purpose of the checklist is to assist U.S. Army commands and agencies in evaluating key management controls outlined below, but not all controls.

B-3. Instructions

The checklist below must be based on the actual testing of key management controls, such as document review, direct observations, and FORDTIS database checks. Identified deficiencies must be explained and corrective action cited in supporting documentation. The key management controls must be officially evaluated at least every 5 years. Commands and agencies shall use DA Form 11-2-R, Management Control Evaluation Certification Statement, to certify the conduct of the evaluation.

B-4. Test Questions

a. Has the Foreign Disclosure Officer (FDO) been appointed in writing? Has copy been provided to the MACOM? (AR 380-10, para 2-11a)

b. Does the FDO have copies of the required publications and documents? (AR 380-10, appendix A)

(1) AR 34-1, International Rationalization, Standardization and Interoperability

(2) AR 55-46, Travel Overseas

(3) AR 70-58, International Professional Scientists and Engineers Exchange Program. (Note. Only required for commands and agencies participating in the program)

(4) AR 380-5, Department of the Army Information Security Program

(5) AR 550-51, International Agreements

- (6) AR 614-10, US Army Personnel Exchange Program With Armies of Other Nations; Short Title: Personnel Exchange Program (Note. Only required for commands and agencies participating in the program)
- (7) DODD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations
- (8) DODD 5230.20, Visits, Assignments, and Exchange of Foreign Nationals
- (9) DODD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure
- (10) National Disclosure Policy and subsequent updates
- c.* Has the FDO attended the FDO certification course? (AR 380-10, para 2-11b)
- d.* Are foreign representatives certified to the command or agency?
- e.* If required, has the foreign representative been issued a distinct badge identifying him/her as a foreign representative? (AR 380-10, appendices K through O)
- f.* When a foreign representative is given access to a computer network, does the local network administrator place a caveat or marker (country named spelled out) on all outgoing e-mails to identify that person as a foreign visitor? (AR 380-10, para 3-5)
- g.* Are activities that are outside of terms of certification reported to the FDO and HQDA? (AR 380-10, appendices K through O).
- h.* Have DA funds or resources been expended to support the activities of foreign representatives visiting or certified to DA? Are the expenditures authorized by and consistent with applicable U.S. law? (AR 380-10, appendix J, para J-10)
- i.* Does the Contact Officer (CO) maintain DDLs or equivalent disclosure documents on all foreign representatives assigned to him/her? (AR 380-10, appendices K through O)
- j.* Has the CO attended the Disclosure Certification Course? (AR 380-10, para 2-11b)
- k.* Are CO designated in writing to control the activities of foreign visitors? (AR 380-10, appendices K through O)
- l.* Has the FDO briefed the CO on their duties? (AR 380-10, appendices K through O)
- m.* Has the CO briefed the foreign representative on DA and local policies affecting the person's status and performance of functions? (AR 380-10, appendices K through O)
- n.* Does the CO brief personnel who have official contact with foreign representatives assigned to the activity? (AR 380-10, appendices K through O)
- o.* Does the CO forward a copy of the certification statement through the FDO to HQDA? (AR 380-10, appendices K through O)
- p.* Does the CO have daily contact with assigned foreign nationals under their respective responsibility? (AR 380-10, appendices K through O)
- q.* Are DDLs or equivalent disclosure documents prepared for each assigned foreign representative? (AR 380-10, appendices K through O)
- r.* Are DDLs or equivalent disclosure documents being maintained for all international programs requiring the disclosure of classified information? (AR 380-10, appendix E)
- s.* Are DDLs coordinated with the host agency network administrator when the foreign visitor requires computer access to ensure that the proposed access is limited to only that information releasable to the foreign representative's government? (AR 380-10, para 3-5)
- t.* Has the FDO disseminated the HQDA approved DDL to all concerned offices within and external to the command or agency, to include the CO? (AR 380-10, appendix E)
- u.* Are disclosures based on a DDL or equivalent document? (AR 380-10, para 2-10)
- v.* Are FORDTIS entries being made for CMI releases within 20 days of the actual first time disclosure? (AR 380-10, para 3-10b)
- w.* Did the command or agency obtain appropriate written authorization when disclosing U.S. CMI classified by another original classification authority? (AR 380-10, para 2-9)
- x.* Does the proponent of the documentary CMI approved for disclosure certify to the FDO that data to be disclosed has been appropriately sanitized? (AR 380-10, para 3-8)
- y.* Prior to any Commerce Business Daily announcement of Requests for Proposals (RFPs) that require the release of CMI, or that will generate CMI (DD 254 attached), is the command's acquisition officer ensuring that: 1) the FDO has approved or obtained approval for foreign participation, and 2) release of the RFPs to eligible foreign participants is occurring through the FDO? (AR 380-10, appendix H, para H-4)
- z.* Is the FDO reviewing munitions license applications to ensure policy compliance? (AR 380-10, appendix I, para I-5)
- aa.* Are FORDTIS visit requests being answered by the HQDA imposed suspense date?
- bb.* Do FORDTIS request of visit authorization (RVA) approval recommendations include, at a minimum: the name and duty phone number of the CO and or Point of Contact, DDL number, international or functional agreement and, advance coordination instructions for recurring visits? If denial is recommended, is rationale provided? (AR 380-10, appendix J, para J-12d)

- cc.* Are recurring RVAs approved only in support of an approved license, contract, or other government program? (AR 380-10, appendix J, para J-11)
- dd.* Are visit requests to contractor facilities reviewed to ensure that visits not in support of an actual or planned DA program are denied (AR 380-10, appendix J, para J-12)
- ee.* Do COs receive guidance (CO responsibilities) from the FDO regarding classified visits? (AR 380-10, appendix J, para J-14)
- ff.* Are personnel who will have official contact with foreign visitors briefed regarding visit parameters and authorized disclosure levels? (AR 380-10, appendix J, para J-14)
- gg.* Do COs report foreign visitor activities that are outside of terms of the visit to proper authorities? (AR 380-10, appendix J, para J-14)
- hh.* Did the CO discuss responsibilities and duties of your assignment during your initial in-brief and provide you a copy of your job description and signed certification form? (AR 380-10, appendix K through O)
- ii.* Did the CO inform foreign visitor of procedures for requesting information and or visits to other agencies? (AR 380-10, appendix K through O).

B-5. Comments

Appendix C Exceptions to Policy

C-1. Exceptions to the National Disclosure Policy (ENDPs)

- a.* An ENDP request is required when a potential disclosure of CMI—
 - (1) Exceeds National Disclosure Policy-1 (NDP-1) prescribed maximum classification level for which the prospective foreign government or international organization recipient is eligible within the CMI category in question.
 - (2) Does not comply with any of the basic disclosure criteria and conditions prescribed in chapter 2 of this regulation.
- b.* Each proposed ENDP is to be sponsored by the HQDA staff agency proponent for the category of CMI that is predominant in the matter at issue. The sponsoring agency will—
 - (1) Task appropriate agencies to provide the complete requisite supporting rationale or justification to ODCSINT, HQDA, to include compliance with all related NDP-1 policy statements, position on the disclosure of cryptographic or COMSEC and intelligence threat information from the National Security Agency (NSA) and the Intelligence Community, respectively, etc.
 - (2) Obtain HQDA staff concurrence in seeking the ENDP.
 - (3) Forward formal request for an ENDP to be initiated by ODCSINT, HQDA. (Note: When possible, forward copy of completed draft of ENDP format through SIPRNET or by an attached 3½ disk).
- c.* ODCSINT, HQDA will—
 - (1) Prepare the proposed ENDP in final form, as depicted in figure C-1.
 - (2) Coordinate the final ENDP package with the sponsoring HQDA agency prior to submission to the NDPC.
 - (3) The NDPC will issue its decision in a record of action (RA). ODCSINT, HQDA will then effect dissemination of the decision, with accompanying disclosure guidance, to the HQDA proponent, initiator of the request, appropriate MACOM, and USASAC (if applicable), at a minimum.

C-2. Exceptions to DA policy

- a.* An exception is required when a potential disclosure of CMI or a foreign representative visit does not conform to DA-established policies, or the administrative requirements or procedures outlined in this regulation.
- b.* Requests for exceptions to DA policy—
 - (1) Must be submitted by a DA agency or command.
 - (2) Must be submitted through command channels, except in those cases involving PMs under the PEO system.
 - (3) Must be prepared and submitted in written letter or memorandum form, unless the urgency of need necessitates submission in electronic message form.

ODCSINT, HQDA (380-10c)

MEMORANDUM FOR THE CHAIRMAN, NATIONAL DISCLOSURE POLICY COMMITTEE (NDPC), OFFICE OF THE UNDER SECRETARY OF DEFENSE (POLICY)

SUBJECT: Request for Exception to the National Disclosure Policy (ENDP) (Insert country here) (Army NDPC Case Number 2000-00) (U)

1. (*) The Department of the Army (DA) requests (insert either "a continuing" or "a one-time") (insert CLASSIFICATION) (insert one or more NDP categories, each with its designation, for example, "Category 1, Organization, Training, and Employment of Military Forces) information to the Government of (insert country) (remainder of sentence states very concisely why the exception is being requested, for example, 'in furtherance of the possible sale of the (system) to the (country) armed forces or in support of the negotiation of a Data Exchange Agreement pertaining to (technology) . Paragraph to be filled in by ODCSINT, HQDA as LEAD agency with initial requester (that is, PM) as assist.

2. (*) An exception to policy is required because the level of classified information involved exceeds the eligibility levels established in NDP-1, Annex A, for (identify country) (This statement will vary with the situation. Some nations may not be listed at all in the annex, and the sentence can therefore vary in content. Basically, the writer is simply stating why an ENDP is needed.). ODCSINT, HQDA (LEAD); initial requester (ASSIST).

3. (*) An assessment of how each of the disclosure criteria and conditions set forth in Section II (Policy) of NDP-1 (as well as chap 2 of this regulation) will be met as follows:

a. (*) Disclosure is consistent with the foreign policy of the United States (U.S.) toward the Government of (the recipient government) (Cite these policies or objectives, avoiding generalities such as "the recipient cooperates with the U.S. in pursuance of military or political objectives.") The JCS Joint Strategic Planning Document Supporting Analysis (JSPDSA) is a good source document for this entry. The following political and military considerations should be addressed: ODUSA (IA) (LEAD); initial requestor and ODCSINT (ASSIST).

Figure C-1. Format for a request for an ENDP

Political Considerations:

- (1) (*) The potential foreign recipient's support for U.S. foreign policy and political objectives.
- (2) (*) The potential of the transfer to deny or reduce an influence or presence in the country that is hostile to U.S. interests.
- (3) (*) The effects of the regional and global strategic balance if the transfer is approved.
- (4) (*) Whether or not the country has a defense treaty or political agreement with the U.S.
- (5) (*) The political benefits that could accrue to the U.S.
- (6) (*) Whether or not the transfer helps the U.S. to obtain or secure base, transit, and overflight rights or access to strategic locations.
- (7) (*) Other countries to which the U.S. has transferred the item.
- (8) (*) The possible reaction of other countries in the region to the proposed sale.
- (9) (*) Whether or not the U.S. is the first supplier of the item.
- (10) (*) The possibility that the item could fall into the hands of terrorists.
- (11) (*) The impact of the transfer on the country's economy.
- (12) (*) Whether or not the transfer establishes an unfavorable political precedent.

Military Considerations:

- (1) (*) The degree of participation in collective security by the U.S.
- (2) (*) How the transfer would affect coalition warfare in support of U.S. policy.
- (3) (*) How the item would increase the recipient country's offensive or defense capability.
- (4) (*) How the transfer would increase the capability of friendly regional forces to provide regional security to assist the U.S. in the protection of strategic line of communication.
- (5) (*) How the transfer will strengthen U.S. or allied power projection.
- (6) (*) To what extent the transfer is in consonance with U.S. military plans.
- (7) (*) Whether or not the export is consistent with Army regional RSI policy.
- (8) (*) Whether or not the system or item is a force structure requirement.
- (9) (*) Can the country's technology base support the item?
- (10) (*) To what degree the system or item counters the country's threat.
- (11) (*) To what extent the system constitutes part of an appropriate force and systems mix.
- (12) (*) Logistical (maintenance, parts, instruction, personnel, changes, or updates) support that will be required.

Figure C-1. Format for a request for an ENDP—Continued

b. (*) The military security of the U.S. permits disclosure. If equipment or technology is involved, there must be a discussion on the results of a compromise on U.S. operational capability or the U.S. position on critical military technology. Initial requester (LEAD); OASA (ALT) and ODUSA (IA) (ASSIST).

(1) (*) Describe the system. Designate exactly what you are trying to sell or disclose.

(2) (*) What components are classified? What elements are really critical? Does the system or do its components represent a significant advance in the state-of-the-art?

(3) (*) What precedent exists for disclosure of this particular system? What other countries have this system? Are export versions available? Are comparable systems (foreign or domestic) using the same technology already in the marketplace?

(4) (*) Do the program manager (PM) and OASA(ALT) support the disclosure of this system (if not the requester of the ENDP)?

(5) (*) Can the critical technology resident in the system be reverse engineered? If so, what level of effort (in terms of time, funding and manpower) is required based on the technological capability of the foreign recipient?

(6) (*) Is the critical technology resident in the system a priority research and development priority for the foreign recipient? Can the critical technology resident in the system be exploited for use in other weapons development programs of the foreign recipient?

(7) (*) If there is a security classification guide for this system, it should be attached as an enclosure.)

(8) (*) If advanced technology is compromised, will it constitute an unreasonable risk to the U.S. military technology?

c. (*) The Government of (the foreign recipient of the information) will afford the information substantially the same degree of security protection given to it by the United States. ODCSINT (LEAD); ODUSA (IA) (ASSIST). This statement is supported in part by the following--

(1) (*) General Security of Military Information Agreement (GSOMIA): (Cite an existing GSOMIA, including date and any extracts that might be appropriate.)

(2) (*) Industrial Security Agreement: (Same guidance as in (1) above.)

(3) (*) NDPC Security Survey: (Same guidance as in (1) above.)

(4) (*) CIA Risk Assessment: (Same guidance as in (1) above.)

(5) (*) Disclosure Policy Statement: (Same guidance as in (1) above.)

(6) (*) (Add additional information to describe the security situation that pertains to the foreign recipient. You can cite other disclosures of other U.S. CMI to that country as examples of U.S. confidence in the security procedures of that country.)

d. (*) Disclosure will result in benefits to the United States at least equivalent to the value of the information disclosed. Initial requestor (LEAD); ODUSA (IA) (ASSIST).

Figure C-1. Format for a request for an ENDP—Continued

(1)(*) (Is there a quid-pro-quo involved? Describe the information and the value to the United States.)

(2) (*) (Explain how the exchange of military information for participation in a cooperative project will be advantageous to the United States from a technical or military viewpoint.)

(3) (*) (If the development or maintenance of a high degree of military strength and effectiveness on the part of the recipient government will be advantageous to the United States, explain how.)

e. (*) The disclosure is limited to information necessary to the purpose for which disclosure is made. (Add a concise statement explaining exactly what this disclosure involves. If this request involves only the sale of the end item (Category 2 information), then the writer should indicate clearly that disclosure of R&D (Category 3) or Production (Category 4) data is not involved or that documentation will be sanitized.) Initial requester (LEAD); ODUSA (IA) and ODCSINT (ASSIST).

4. (*) Explain any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure schedules, or other pertinent caveats that may affect approval or denial of the request. Limitations include phasing of the disclosure, substitution or removal of components, prohibitions on the disclosure of certain hardware or information, and restrictions that must be included before the disclosure can be executed. It should be noted that if there is no security agreement in force, an item-specific agreement must be executed with the recipient country before the disclosure. The inclusion of a draft DDL may satisfy this requirement. Initial requester (LEAD); OASA (ALT) and ODCSINT (ASSIST).

5. (*) The requested exception is a continuing exception, subject to annual review (or is a one-time exception to expire on a given date). (A continuing exception usually is associated with a long-term project, such as a co-production program or military sale when the U.S. will be obligated to provide life cycle support. A one-time exception typically is used for a briefing or demonstration or short-term training.) Initial requester (LEAD); ODUSA (IA) and ODCSINT (ASSIST).

6. (*) The U.S. country team in (insert country) supports this initiative. (NDP-1, section IV (Procedures) requires that prior to approval of any new disclosure program, or submission of a request for exception to policy, appropriate U.S. officials in the recipient country, as well as the views of the Unified Commander, will be consulted concerning the approval. Attach as an enclosure a copy of the country team message that provides their comments. Sufficient time should be allowed to obtain an opinion from U.S. Embassy personnel in country and the responsible Unified Commander before submitting the request for approval. Many cases are delayed because a U.S. Embassy or Unified Commander opinion has not been obtained.) ODUSA (IA) (LEAD); ODCSINT (ASSIST).

Figure C-1. Format for a request for an ENDP—Continued

7. (*) (Add here the opinion of other interested Departments or Agencies if joint-Service or shared information is involved. If the information or item of equipment is of shared or joint interest, such as an air-to-air missile used by two Services or containing technology of concern to another Service, the views of the other party should be included.) ODUSA (IA) (LEAD); initial requestor, OASA (ALT), and ODCSINT (ASSIST).

8. (*) (Add here any information not mentioned that would assist the NDPC members, the Secretary of Defense, or the Deputy Secretary of Defense in evaluating the proposal. The preparer can use this paragraph to present evidence that would counter arguments (usually involving the security status of the proposed recipient or concerns for the technology involved) opposing the disclosure. The preparer must not attempt to avoid these opposing views but must address and mitigate each issue. If risks associated with the request cannot be completely avoided, a plan to manage and minimize the risks should be developed. Failure to do so may result in an adverse reaction to the case when these issues are eventually raised.) Initial requestor (LEAD); ODUSA (IA) (ASSIST).

9. (*) Points of Contact (POCs): The name and telephone number of knowledgeable individuals within the requesting organization who can provide additional technical detail or clarification concerning the case at issue. Initial requestor (LEAD); ODUSA (ASSIST). Usually the following are included--

a. (*) (Name, rank (if military), office symbol, and telephone number of the sponsor or preparer.)

b. (*) (Name, rank (if military), office symbol, and telephone number of the PM, OASA(ALT) official, and technical expert on the system at issue, as applicable.)

c. (*) (Name, rank (if military), office symbol, and telephone number of the ODCSOPS and ODCSINT action officer who provided input to the political-military and risk assessments for this case.

d. (*) (Name, rank (if military), office symbol, and telephone number of the Army member (or alternate), NDPC, who submits the case to the NDPC.

10. (*) An NDPC vote is requested no later than (insert date) (Ten full working days for NDPC case deliberations should be allowed. The suspense date (10 full working days) is computed starting from the first full working day after the date of the request.)

Encls

Signature Block
LTC, GS
Army Member, NDPC

(RECOMMENDED ENCLOSURES: Country team message, security classification guide, or other applicable technical assessment for the item or equipment proposed for export, and any other enclosures necessary to understanding the case.)

* Insert the highest security classification level for the information contained in the paragraph or subparagraph.

Figure C-1. Format for a request for an ENDP—Continued

Appendix D

Technology Assessment/Control Plan (TA/CP)

D-1. Overview

a. The TA/CP requirements set forth in paragraphs D-1b through D-1d below meet the technology assessment prerequisite for requests for authority to negotiate (RAN) an international agreement under AR 550-51. In developing the TA/CP, cognizant DA activities will consider and incorporate, as appropriate, all applicable NDP-1 and DOD technology transfer policy guidelines, and Army disclosure policy.

b. After HQDA review and approval, the TA/CP will be used by the cognizant DA component as the basis for developing negotiating guidance prior to negotiations with a foreign government.

c. The TA/CP also requires that the cognizant DA activity develop a DDL as part of a request for authority to conclude (RAC) an agreement. The DDL will provide detailed guidance regarding disclosures of all elements of the system, information or technology in question. Until the DDL has been approved, there can be no promise or actual disclosure of sensitive information or technology. For phased R&D programs, both the TA/CP and the DDL should address time-phased disclosures of technical data to ensure that sensitive information is protected from premature or unnecessary exposure.

d. The DDL also will provide specific and detailed guidance to support evaluation of proposed exports/disclosures of defense articles and technical documents by DA Components and defense contractors. The format in appendix E may be used as general guidance for the preparation of DDLs.

e. Upon conclusion of an agreement, the DDL will be updated (as required) and issued by ODCSINT, HQDA to ensure that transfers of defense articles and information by USG or U.S. industry personnel comply with the TA/CP, NDP-1, and applicable DOD/Service security policies and procedures.

D-2. Program concept

Briefly describe the basic concept of the proposed subject of the agreement. The description will be in terms of the overall technical, operational, and programmatic concept, including, as appropriate, a brief summary of the requirement or threat addressed. If possible, use official military designations. When applied to R&D cooperative programs not related to specific systems, the technical objectives and limits of the cooperative effort should be defined.

D-3. Nature and scope of effort/objectives

State the operational and technical objectives of the proposed subject agreement. Indicate specifically the following—

- a.* Nature and scope of the activity (for example, cooperative research, development, and or production).
- b.* Country or country groups participating, and the anticipated extent of participation by each, including identification of foreign contractors and subcontractors, if known. Differentiate between those that are committed participants and those that are only potential participants.
- c.* Program phases involved and, if applicable, quantities to be developed and produced or tested.
- d.* Summary of projected benefits to U.S. and other participants: technology, production bases, and military capability.
- e.* Cognizant POCs within DA Component headquarters or program management organization.
- f.* Major milestones or dates by which the assessment will require review or revision.

D-4. Technology assessment

a. Identify products or technologies involved in the program. This section of the assessment should discuss topics listed below using the MCTL and other applicable DOD/Service technology transfer policies as guides. The FDO is the PM's link to the intelligence community for threat, foreign intelligence, and other supporting intelligence/security data.

- (1) Design and manufacturing know-how and equipment used for development and production.
- (2) Systems or components or information used for other purposes (for example maintenance or testing) that would allow a recipient to achieve a major operational advance. (When applicable, cite other specific U.S. programs and projects from which technical information or hardware will be provided.)

b. State classification and NDP category (such as Category 3 (R&D)) of U.S. technical data and design and manufacturing know-how to be contributed.

c. Provide an evaluation of the foreign availability of comparable systems (considering quality, production capability and costs, if known) and comparable/competing technologies, including—

- (1) Current or projected capabilities worldwide;

- (2) Current or projected capabilities of proposed participants or recipients; and
- (3) Availability of technologies worldwide.
- d.* Identify any previous disclosures or current programs (such as sales, cooperative programs, information exchange) involving the transfer or exchange of this or comparable equipment and technologies.
- e.* Describe the impact on U.S. and foreign military capability as a result of participation in this program:
 - (1) Identify and describe the extent to which the U.S. system or technology contributes to an advance in the state-of-the-art, or a unique operational advantage. Include, if known, a summary of U.S. investment and R&D or operational lead-time represented.
 - (2) State the specific contribution of foreign participants to program objectives, project resources, and enhancement of the U.S. military capability and technology base.
- f.* Describe the potential damage to the U.S. technology position and military capability in the event of a compromise (without regard to potential participants). Explicitly address the impact of loss or diversion of the system or technology. Specify assumptions and discuss the following—
 - (1) Transfer of a military capability the loss of which would threaten U.S. military effectiveness (for example, a missile seeker for which we have no countermeasures, or information allowing the development of effective countermeasures negating a primary U.S. technological advantage).
 - (2) Potential compromise of sensitive information revealing systems' weaknesses that could be exploited to defeat or minimize the effectiveness of U.S. systems;
 - (3) Susceptibility to reverse engineering of sensitive design features or fabrication methods;
 - (4) Extent to which the technology that is to be transferred can be diverted and or exploited for purposes other than the one intended under the specific program (for example, a technological capability to fabricate ring laser gyros translates into an ability to implement advanced long-range missiles, precision land and sea navigation, etc.); or
 - (5) Potential impacts of participation on U.S. competitive position or U.S. industrial base, if any. (The conclusions of the Industrial Base Factors Analysis may be incorporated by reference.)
- g.* Estimate the risk of compromise, considering the following—
 - (1) Susceptibility of the technology to diversion or exploitation, and its priority as a target for foreign intelligence service (FIS) collection, if known. (The degree of susceptibility will depend to a great extent on the exact nature of the technology in question, the form of the transfer, and the indigenous capability of the recipient);
 - (2) The potential participants/recipients, including—
 - (a) An evaluation of their security and export control programs (including reference to any specifically related agreements with the U.S.).
 - (b) Their past record of compliance with such agreements and in protecting sensitive/classified information and technology.

D-5. Control Plan

This section of the TA/CP is the basis for negotiating guidance for agreements. The DDL implements the disclosure aspects of the control plan. Specifically, this section will identify measures proposed to minimize both the potential risks and damage due to loss, diversion, or compromise of the critical, classified elements and will clearly identify any specific limitations/conditions required to protect unique U.S. military operational and technological capabilities. Appropriate measures that should be considered and discussed include—

- a.* Phased disclosure of information to ensure that information is disseminated only when and to the extent required to conduct the program. (Specifically, production technology should not be disclosed prior to a program decision requiring the use of the technology in question.);
- b.* Restrictions on disclosures of specific information to protect U.S. national security interests. Be specific with regard to details of design and production know-how and software, including software documentation, development tools and know-how;
- c.* Transfer of specific hardware or software components in modified form, or as completed, tested items;
- d.* Special security procedures (both government and industrial) to control access to restricted materiel and information. Also to be considered are—
 - (1) Controls on access of foreign nationals at U.S. facilities; and
 - (2) Procedures to control disclosures by U.S. personnel at foreign facilities; and
- e.* Other legal or proprietary limitations on access to and licensed uses of the technology in implementing technical assistance agreements.

D-6. Notes

- a.* In some cases, particularly early in R&D programs, the full range of technological alternatives and potential participants may not be fully known. Specific hardware and technical data may not be completely defined, and the nature and availability of end items and technical data can evolve rapidly during a development program. In these

cases, the TA/CP should define comprehensive technical criteria, in sufficient detail to support disclosure decisions as the program evolves.

b. The TA/CP should be supported by detailed evaluation of the individual elements of hardware and technical data relating to the program. With this supporting information, the resulting document should be adequate to support any case-by-case evaluation required for program implementation, including commercial and government sales, co-production, and information exchange programs.

c. The TA/CP is a “living” document, subject to continuous review and appropriate update. A product improvement proposal (PIP) usually constitutes a major improvement to a given weapon system and therefore a concomitant update to the TA/CP would normally be required. This update to the TA/CP is critical for those personnel conducting the daily functions of the U.S. Army’s international cooperative and foreign disclosure/international technology transfer programs.

Appendix E

Delegation of Disclosure Authority Letter (DDL)

E–1. General

A DDL is a document issued by the appropriate Designated Disclosure Authority describing classification levels, categories, scope, and limitations related to information under Army’s disclosure jurisdiction that may be disclosed to specific foreign governments or their representatives for a specified purpose. ODCSINT, HQDA approves and issues DDLs for classified programs or projects regarding the following—

- a.* International Agreements.
- b.* FLO (Position DDLs).
- c.* Army Personnel Exchange Programs (ESEP (Individual DDLs), and MPEP and CPPs (Position DDLs)).
- d.* Weapon Systems.
- e.* Organizational (commands and agencies).
- f.* Cooperative R&D (that is, DEAs, Technology R&D Programs (TRDPs), etc.). DA elements will coordinate, to include lateral coordination, all DDLs prior to submission to ODCSINT, HQDA for approval. ODCSINT, HQDA will distribute the approved DDLs to all affected offices within HQDA and the appropriate MACOM(s). Upon receipt of approved DDLs, FDOs should effect internal Army dissemination of the DDLs to all affected parties, such as contact officers, PMs, subject matter experts, USASAC, training and doctrine elements, operational units with weapons system in their inventory.

E–2. Warning statement

The data elements contained in the following sample formats (see figs E-1 and E-3) must be used by DA elements to develop a DDL. As early as possible in the process, the initiator of the international proposal, the FDO, and the subject matter experts will collectively develop the DDL. The FDO will be responsible for ensuring that all pertinent disclosure questions concerning the proposal are raised and answered. From an administrative perspective, each DDL requires a warning statement stipulating that the DDL is an internal U.S. Army document, which is not to be divulged, in total or in part, to any foreign government or foreign government representative. This warning statement is to be placed at the top of each page and the bottom of the last page of the DDL. The warning statement must be bold and in larger letters than the contents of the document so it clearly stands out. The exact wording of the warning statement is cited in the sample formats.

E–3. Unclassified DDLs

Unclassified DDLs may be transmitted by U.S. mail, facsimile, International Agreements Tracking System (IATS), or over the NIPPRNET (DOD’s U.S.-only unclassified network and e-mail). ODCSINT, HQDA encourages the use of NIPRNET, IATS, or 3 1/2 inch disk for the transmission of all completed unclassified draft DDL formats.

E–4. Approval

A HQDA-approved DDL is required to be in place prior to a commitment to assign a FLO, foreign exchange personnel, or CPP to a DA component.

E–5. Requirement

According to DODDs 5230.11 and 5230.20, an equivalent document containing data elements of a DDL is required for all unclassified U.S. Army weapon systems, international agreements, and FLO, StanRep, MPEP, ESEP, and CPP positions necessitating access to only unclassified information. The local commander may approve this document with a copy furnished to ODCSINT, HQDA.

THE INFORMATION CONTAINED IN OR A COPY OF THIS DDL
WILL NOT BE PROVIDED TO THE SUBJECT OF THIS DDL OR
ANY OTHER FOREIGN NATIONAL

OFFICE SYMBOL (380-10)

DDL APPROVAL NUMBER: 001-99

DDL APPROVAL DATE: 01/01/99

DDL EXPIRATION DATE: This DDL will be in effect indefinitely or until the scope is changed.

SUBJECT: Delegation of Disclosure Authority Letter (DDL) - NAME OF WEAPON SYSTEM

1. CLASSIFICATION: The highest level of CMI that may be disclosed is (INDICATE HIGHEST SECURITY CLASSIFICATION LEVEL AUTHORIZED FOR DISCLOSURE.)

2. DISCLOSURE METHODS: INDICATE TYPES OF DISCLOSURE METHODS AUTHORIZED. For example: Oral, Visual, and/or Documentary.

3. CATEGORIES PERMITTED: USE CHAPTER 2 OF THIS REGULATION AS A GUIDE, INDICATE THE OF CMI AUTHORIZED FOR DISCLOSURE.

4. SCOPE: INDICATE CLEARLY TO WHOM THE DISCLOSURE AUTHORITY IS GRANTED, FOR WHAT SYSTEM. For example, The Commander, AMCOM is delegated authority to disclose CMI originated by AMCOM and the Apache PM (with the concurrence of the Apache PM) within the categories listed in paragraph 3, subject to the limitations delineated in paragraphs 5 and 6. The Commander may also disclose CMI originated outside of AMCOM and the Apache PM Office when the disclosure is authorized in writing by the originator of the CMI and is within the scope of this DDL. Note: The originator or proponent for CUI is the disclosure authority for that information. The Governments of X, Y and Z (BASED ON ARMY EXPORT POLICY)

Figure E-1. Sample format of DDL for weapons system

5. AUTHORIZED FOR DISCLOSURE:

IN GENERAL, DISCLOSURES OF CMI ARE INCLUSIONARY, NOT EXCLUSIONARY, WITH REGARD TO THE WEAPON SYSTEM PURCHASED. CMI AUTHORIZED FOR DISCLOSURE TO A FOREIGN CUSTOMER INCLUDES ALL INFORMATION REQUIRED FOR THE OPERATION, TRAINING, EMPLOYMENT, AND MAINTENANCE OF THE CONFIGURATION OR VERSION OF THE U.S. ARMY WEAPON SYSTEM PURCHASED, EXCLUDING THAT INFORMATION, MATERIEL, OR CAPABILITY CITED IN PARAGRAPH 6.

IN THIS PARAGRAPH, CLEARLY STATED WHAT INFORMATION UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY IS/WILL BE AUTHORIZED FOR DISCLOSURE. IT IS IMPORTANT THAT THE DA COMMAND OR AGENCY DEVELOPING THE DDL BE AS DETAILED AS POSSIBLE. THIS PARAGRAPH SHOULD PROVIDE SPECIFIC DETAILS REGARDING THE INFORMATION TO BE DISCLOSED, TO INCLUDE THE LEVELS OF THE CLASSIFICATION ANTICIPATED FOR DISCLOSURE AT DIFFERENT PHASES OF THE PROGRAM. TERMINOLOGY USED MUST BE CONSISTENT WITH THAT USED IN THE DEVELOPMENT OF THE APPLICABLE SYSTEM SECURITY CLASSIFICATION GUIDE. THE SECURITY CLASSIFICATION GUIDE FOR A WEAPONS SYSTEMS OR TECHNOLOGY PROVIDES A COMMON LANGUAGE AND FRAMEWORK FOR DEVELOPING PARAGRAPHS 5 AND 6. IT IS RECOMMENDED THAT THE LANGUAGE IN THE GUIDES AS WELL AS THE TOPICAL SUBDIVISIONS IN THE GUIDE BE USED AS A TEMPLATE FOR STRUCTURING PARAGRAPHS 5 AND 6. INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS WILL UNNECESSARILY DELAY THE STAFFING PROCESS. FOR EXAMPLE:

PHASE I -- FOREIGN CUSTOMER DECISION PHASE

- This phase covers preliminary discussions with prospective customers regarding end items sales, co-production, and co-assembly through FMS and/or DCS. A pre-sale information package includes all information necessary for a prospective customer to make a purchase decision regarding a specific U.S. Army weapons system. This package should address and may include information, such as general weapons system performance characteristics and capabilities, technical specifications, P&A data, maintenance and training. Preliminary disclosures are generally limited to the CONFIDENTIAL security classification level.

Figure E-1. Sample format of DDL for weapons system—Continued

PHASE II – FOREIGN CUSTOMER DECISION TO BUY PHASE

- This phase begins upon receipt of a commitment to buy, signed contract, or MOU. A post-decision information package includes all information necessary for the purchaser to operate, train, employ, and maintain the configuration of the U.S. Army weapon system purchased. This package should address and may include information, such as specific weapons system performance characteristics and capabilities, technical specifications, maintenance (depot) and training, DCS procedures and disclosure guidance, software, etc. at the SECRET security classification level.

Note: The information packages cited above should be resident in the U.S. Army export policy regarding each classified, major U. S. Army weapons system. The export policy should also address the specific configuration of the U.S. Army weapons system regarding each classified sub-component that the U.S. Army is willing to transfer to any allied or friendly, non-allied country.

Note: Figure E-2 is a graphic portrayal with specific references to conditions and limitations of the configurations and CMI associated with a U.S. Army weapons system that is authorized for transfer to a specific foreign government or international organization.

6. NOT AUTHORIZED FOR DISCLOSURE:

IN GENERAL, DISCLOSURES OF CMI ARE INCLUSIONARY, NOT EXCLUSIONARY, WITH REGARD TO THE WEAPON SYSTEM PURCHASED. HOWEVER, THERE ARE SPECIFIC CMI, MATERIEL, OR CAPABILITY THAT MAY NOT BE AUTHORIZED FOR DISCLOSURE TO ANY INDIVIDUAL FOREIGN CUSTOMER OR ANY GROUP OF FOREIGN CUSTOMERS, REGARDLESS OF THE REQUIREMENT TO PROVIDE FOR OPERATIONAL, TRAINING, EMPLOYMENT, AND MAINTENANCE INFORMATION CONCERNING THE CONFIGURATION OR VERSION OF THE U.S. ARMY WEAPON SYSTEM PURCHASED.

THIS PARAGRAPH MUST SPECIFY THE LIMITS OF THE DISCLOSURE AUTHORITY. PARTICULAR ATTENTION MUST BE PAID TO THE CPI IDENTIFIED IN THE U.S. ARMY WEAPON SYSTEM, AS A MINIMUM. IN ADDITION, CPI THAT WAS LEVERAGED FROM ANOTHER U.S. ARMY WEAPON SYSTEM MUST BE COORDINATED WITH THE APPROPRIATE PM AND PROTECTED ACCORDINGLY. AGAIN, INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS. AT A MINIMUM, THE FOLLOWING INFORMATION SHOULD BE INCLUDED--

Figure E-1. Sample format of DDL for weapons system—Continued

The following CMI is not authorized for disclosure under the terms of this DDL. Requests for exception to these restrictions must be forwarded through foreign disclosure channels to HQDA.

a. GENERAL:

(1) Detailed information to include discussions, reports and studies of system capabilities, vulnerabilities and limitations which leads to conclusions on specific tactics or other countermeasures, that would otherwise not be assumed, that will defeat the system.

(2) Electromagnetic signatures (if applicable to specific system or portion of a system).

(3) Acoustic signatures (if applicable to a specific system or portion of a system).

(4) Low Observable requirements or Advanced Signatures Data.

(5) Non-Cooperative Recognition Data.

b. SPECIFIC: SPECIFIC ITEMS LISTED AS NOT AUTHORIZED FOR DISCLOSURE MUST BE INDICATED AT THE SAME LEVEL OF DETAIL AS IN PARAGRAPH 5 ABOVE. INFORMATION THAT WAS CLASSIFIED UNDER THE ORIGINAL CLASSIFICATION AUTHORITY OF AN INDIVIDUAL/AGENCY OTHER THAN THE DELEGATION AUTHORITY SPECIFIED IN THIS DDL IS NOT AUTHORIZED FOR DISCLOSURE WITHOUT THE WRITTEN APPROVAL OF THAT INDIVIDUAL/AGENCY.

7. PROCEDURES: THE FOLLOWING INFORMATION (AT A MINIMUM) MUST BE INCLUDED IN THIS PARAGRAPH: The following procedures will be used concerning disclosure decisions on CMI under the terms of this DDL.

The following procedures will be followed concerning the disclosure or denial of CMI authorized under the terms of this DDL.

a. All CMI disclosure decisions will be consistent with this DDL, comply with the "Need-to-Know" principle, and take into account the level of foreign (IDENTIFY) government involvement in the (LIST PROGRAM, STUDY, SYSTEM INVOLVED). CMI disclosure will be limited to the minimum level of classification and detail necessary to accomplish the specific purpose of the disclosure.

Figure E-1. Sample format of DDL for weapons system—Continued

b. APPLICABLE ONLY FOR DOCUMENTATION WHICH MAY BE REQUESTED BY A FLO OR HIS GOVERNMENT. Transfer of classified documents to foreign (IDENTIFY) government representatives will be processed through government-to-government channels. For the purposes of this DDL, (IDENTIFY) is authorized/not authorized to receipt for CMI identified for disclosure to his or her government.

c. Records of CMI Disclosure Decisions:

(1) Authorized representatives (IDENTIFY BY TITLE SUCH AS CONTACT OFFICER OR POSITION WITHIN THE COMMAND) who disclose CMI (oral, visual, or documentary) to foreign (IDENTIFY) officials WILL record the disclosure (using DD Form 1822, Report of Disclosure or Denial of U.S. CMI) and forward the record to the nearest supporting foreign disclosure office, (SPECIFY WHERE DISCLOSURE RECORD IS TO BE FORWARDED, THAT IS, SECURITY DIVISION, INSTALLATION SUPPORT ACTIVITY, ETC) when one of the following occurs--

(a) First-time disclosures based on one of the following--new information or new (higher) classification level.

(b) The disclosure of information that extends the scope or detail of previously-disclosed information.

(c) The authorized disclosing representative will ensure that all disclosures fitting any of the above categories and the terms of this DDL are reported using the DD Form 1822.

(2) The office responsible for the FORDTIS database will enter the disclosure decision into the FORDTIS database.

(3) If a FORDTIS terminal is not available, the DD Form 1822 will be reviewed for completeness by the supporting FDO and forwarded to the next echelon possessing a FORDTIS capability. Instructions for data entry are in DOD 5230.18M, The FORDTIS Users Manual.

THE INFORMATION CONTAINED IN OR A COPY OF THIS DDL
WILL NOT BE PROVIDED TO THE SUBJECT OF THIS DDL OR
ANY OTHER FOREIGN NATIONAL

Figure E-1. Sample format of DDL for weapons system—Continued

SAMPLE FOREIGN DISCLOSURE GUIDELINE SUMMARY COUNTRY XYZ

	CLASS	END ITEM	END ITEM	END ITEM	ACQUISITION	LEVEL OF MAINTENANCE	
		RELEASABLE	PURCHASED	RESTRICTION	CATEGORY	"Y" LEVEL	"D" LEVEL
AIRFRAME							
AH-64A APACHE AIRCRAFT	S	Y	Y	1.0	Inventory	Y	Y
AH-64D APACHE AIRCRAFT	S	Y	N	1.0	Production	Y	Y
LO APPLICATIONS	S	Y	Y	2.2			
RADAR CROSS SECTION (RCS)	S	Y	Y	2.3			

EXAMPLE ONLY

UNCLASSIFIED

Figure E-2. Sample matrix

	CLASS	END ITEM		ACQUISITION	END ITEM	LEVEL OF MAINTENANCE	
		RELEASE	PURCHASED			CATEGORY	RESTRICTION
AIRFRAME							
AH-64A Apache Helicopter	S	Y	Y	Production	1.0	Y	N
AH-64D Apache Helicopter	S	Y	N	Production	1.0	Y	N
RADAR CROSS SECTION (RCS)	*	Y	Y		2.1	NA	NA
LD APPLICATIONS	S	Y	Y			Y	N
COMPUTERS							
MISSION COMPUTER (MC)							
ADVANCED MISSION COMPUTER	U		Y	Production	2.2	Y	N
CONTROLS AND DISPLAYS							
Heads-Up Display							
	U		Y	Production		Y	N
Digital Mapping System	U		Y	Production	2.3	Y	N
NAVIGATION AND FLIGHT AIDS							
INERTIAL NAVIGATION SYSTEM (INS)							
	U		Y	Production		Y	N
EMBEDDED GLOBAL POSITIONING SYS (GPS)							
PPS	S		Y	Production	2.4		N
SPS	U		Y	Production	2.4		N
OTHER NAV AND FLIGHT AIDS							
STANDBY COMPASS	U		Y	Production		Y	N
RADAR ALTIMETER SET	U		Y	Production		Y	N
MAGNETIC AZIMUTH DTC	U		Y	Production		Y	N
ANGLE OF ATTACK INDICATOR	U		Y	Production		Y	N
ELECTRONIC FLIGHT CONTROL							
ELECTRONIC FLIGHT CONTROL SYSTEM							
	U		Y	Production		Y	N
TACTICAL SENSORS							
RADAR							
AN/APG-78 FIRE CONTROL RADAR (FCR)	S		Y	Production	2.5	Y	Y
AN/APR-48 FREQ INTERFEROMETER (RFI)							N
AN/APR-289 RADAR ALTIMETER SET	U		Y	Production		Y	N
AN/ASB-167 DOPPLER SENSOR	U		Y	Production		Y	N
FLIR							
FLIR WLTD	S		Y	Production	2.6	Y	N

Figure E-2. Sample matrix—Continued

	CLASS	END ITEM	END ITEM	ACQUISITION	END ITEM	LEVEL OF MAINTENANCE	
		RELEASE	PURCHASED	CATEGORY	RESTRICTION	'I' LEVEL	'D' LEVEL
NIGHT VISION DEVICES							
TADS (ANASG-173P/WVS (ANAAQ-15))	U		Y	Production		N	N
STORES MANAGEMENT							
ANAYK-1000 SMS and previous version	U		Y	Production		Y	N
ANAYQ-1000(V) Armament Control Processor	U		Y	R&D		Y	N
ANIAWW-17 Elect. Fuze Power Supply	U		Y	Production		Y	N
COMMUNICATION/IDENT.							
RADIOS							
ANARC-164	U		Y	Production		Y	N
TSEC/KY-48 SECURE SPEECH SYSTEM	U		Y	Production		Y	N
ANARC-186	U		Y	Production	2.7	Y	N
ANARC-381(D) VHF	U		Y	Production		Y	N
AM-7188ARC RF AMPLIFIER	U		Y	Production		Y	N
ANARC-329 HF	S		Y	Production		Y	N
DM591-302 IMPROVED DATA MODEM	U		Y	R&D		Y	N
IFF							
ANAPX-505	U		Y	Production		Y	N
TSEC KIT-1A AND 1C	S		Y	Production		N	N
ELECTRONIC WARFARE							
BEX-898HA INTR BLANKER	U		Y	Production		Y	N
BCM							
ANALG-2069 RF COUNTERMEASURES (RFCM)	S		N	R&D			
JAMMERS							
ANALQ-136 RADAR JAMMER	S		Y	Production	2.4	Y	N
ANALQ-144 IR COUNTERMEASURE SYSTEM	S		Y	Production	2.8	Y	N
CHAFF/DECOYS/FLARES							
M-130 GP CHAFF DISPENSER	S		Y	Production	2.9	N	N
RWR							
ANAPR-26A	S		Y	Production		Y	N
ANALR-2A LASER DETECTOR SET	S		Y	Production		Y	N

Figure E-2. Sample matrix—Continued

	CLASS	END ITEM	END ITEM	ACQUISITION	END ITEM	LEVEL OF MAINTENANCE	
		RELEASE	PURCHASED	CATEGORY	RESTRICTION	"D" LEVEL	"C" LEVEL
RECORDING/MONITORING							
AN/ASQ-8000 FIRAMS	U		Y			Y	Y
VIDEO CAMERAS							
MX-12347-ASQ VIDEO CAMERA	U		Y			Y	Y
TCS-8889 HUD COLOR CAMERA	U		Y			Y	Y
RECORDERS							
TEAC-V-8888 AB-RVS	U		Y			Y	Y
SVCB-V777 COLOR	U		Y			Y	Y
POWER PLANTS							
ENGINES							
T780-GE-701	S		Y			Y	Y
T780-GE-701C	S		Y			Y	Y
WEAPONS Air to Air							
STINGER	S		Y	Production	2.10	N	N
WEAPONS Air-to-GROUND							
HELLFIRE	S		Y		2.11	N	N
HELLFIRE II	S		Y		2.12	N	N
2.75" ROCKET	S		Y		2.13	Y	Y
TRAINING EQUIPMENT							
SIMULATOR	U		Y	Production	2.14	Y	N/A
SOFTWARE SOURCE CODE							
COMPUTER PROCESSOR	C		Y		UNCLASSIFIED ONLY	Y	N/A
DIGITAL DISPLAYS	U		Y		UNCLASSIFIED ONLY	Y	N/A
COMM. SYS. CONTROLLER	U		Y		UNCLASSIFIED ONLY	Y	N/A
AN/APG-65	S		N		2.15		
AN/APR-39(V) RWR	S		N		2.15		
AN/ALQ-144 IRCM	S		N				
AN/ALQ-136 RADAR JAMMER	S		N				
SIMULATOR	U		Y			Y	N/A
OPERATIONAL TEST SET	U		Y		2.16	Y	N/A

Figure E-2. Sample matrix—Continued

COUNTRY XYZ

FOREIGN DISCLOSURE GUIDELINES FOR

AH-64 APACHE HELICOPTER

(U) The conditions and limitations cited below applies to the transfer of the AH-64 Apache Helicopter to Country XYZ. The conditions and limitations in general section (paragraph 1.0) apply, as appropriate, in the absence of specific conditions and limitations in the specific section (paragraph 2.0). In the event of a conflict between conditions and limitations in the general and specific sections, the conditions and limitations in the specific sections will prevail.

1.0 (U) GENERAL CONDITIONS AND LIMITATIONS

- a. (U) Prior to a decision to purchase the AH-64 Apache, information that may be disclosed will be limited to general weapons system performance characteristics and capabilities, technical specifications, P&A data, and maintenance and training at the CONFIDENTIAL security classification level. Sales will be through FMS channels. Co-production and co-assembly is not authorized.
- b. (U) After a decision to purchase is made, SECRET information may be disclosed regarding operations, training, employment, and maintenance of the configuration of the U.S. Army weapon system purchased.
- c. (U) Depot-level maintenance is not authorized for release.
- d. (U) Intelligence or threat information marked "NOT RELEASABLE TO FOREIGN NATIONALS" (NOFORN).
- e. (U) Information under the cognizance of another Military Department.
- f. (U) Propriety information owned by a private firm or citizen.
- g. (U) Information obtained from a foreign government unless the foreign government authorizes the disclosure, in writing, to a third party.
- h. (U) Detailed information to include discussions, reports and studies of system capabilities, vulnerabilities and limitations which leads to conclusions on specific tactics or other countermeasures, that would otherwise not be assumed, that will defeat the system.

Figure E-2. Sample matrix—Continued

i. (U) Electromagnetic signatures (if applicable to specific system or portion of a system).

j. (U) Acoustic signatures (if applicable to a specific system or portion of a system).

k. (U) Low Observable requirements or Advanced Signatures Data.

l. (U) Non-Cooperative Recognition Data.

2.0 (U) **SPECIFIC CONDITIONS AND LIMITATIONS**

2.1 (U) **Radar Cross Section (RCS)**

a. (*) Test for measuring RCS will be on a USG range and controlled by the U.S. Army.

b. (*) Configuration of the Apache to be measured will include only those weapons systems in the inventory of Country XYZ.

c. (*) Results of the test will be classified according to the instructions of Country XYZ.

2.2

2.3

2.4

2.5 (U) **AN/APG-78 Fire Control Radar**

a. (*) Depot-level maintenance is not authorized.

b. (*) ECM techniques are not authorized for disclosure.

c. (*) Classified software source code.

* Fill in the correct security classification.

Figure E-2. Sample matrix—Continued

DEVELOPMENT OF DISCLOSURE GUIDANCE FOR MAJOR, CLASSIFIED U.S. ARMY WEAPONS SYSTEMS

The procedures outlined below relate to the development of disclosure guidance for major, classified U.S. Army weapons systems.

Procedures:

- Step 1:** The development of the Program Protection Plan (PPP) no later than Milestone I of the acquisition process should “trigger” the commencement of the U.S. Army’s export policy for the weapons system. The primary document that contributes to the development of the export policy is the technology assessment and control plan (TA/CP), which is annex to the PPP.
- Step 2:** The development of the U.S. Army export policy should include the following:
- Army willingness to transfer the weapons system to individual or groups of foreign countries.
 - Army willingness to transfer specific versions of the weapons system to individual or groups of foreign countries.
 - Citation of general and/or specific conditions and limitations associated with the weapons system to include its components and munitions.
 - Pre-sale information package regarding possible sales, co-production, and co-assembly that the U.S. Army has determined is required by a prospective customer to make a purchase decision. This package should address and may include information, such as general weapons system performance characteristics and capabilities, technical specifications, P&A data, maintenance and training, sales through FMS or DCS channels, and co-production authorization. This information will generally be limited to the CONFIDENTIAL security classification level.
 - Post-decision information package includes data that a prospective customer requires to operate, train, employ, and maintain the configuration of the U.S. Army weapon system purchased. This package should address and may include information, such as specific weapons system performance characteristics and capabilities, technical specifications, maintenance (depot) and training, DCS procedures and

Figure E-2. Sample matrix—Continued

disclosure guidance, software, etc. at the SECRET security classification level (maximum).

- Based on the approved U.S. Army export policy, the FDO, in collaboration with the technical and security assistance subject matter experts, may use the attached matrix with general and specific conditions and limitations as a tool to portray graphically the disclosure guidance for the transfer of the U.S. Army weapon system and associated information sold to a specific foreign country.

Step 3: After the approval of the U.S. Army export policy regarding a specific weapons system and the issuance of an approved DDL, as appropriate, HQDA shall disseminate the policy (with DDL) to the appropriate PM and MACOM or agency head. The PM, in collaboration with the FDO, shall disseminate appropriate disclosure guidance (copy of the DDL with the matrix (optional)) to affected U.S. Army elements, such as TRADOC, maintenance depot, U.S. units with the weapons system in their inventory, PMs who are leveraging technologies from the system, and PMs of weapons system(s) from which technologies were leveraged.

Figure E-2. Sample matrix—Continued

Delegation of Disclosure Authority Letter for Foreign Participants in FLO, StanRep, MPEP, ESEP, and CPP Positions *(Note: The DDL outlined below is a position DDL and applies to FLOs, StanReps, MPEP, and CPP participants. The DDL for ESEP participants is an individual DDL. The primary difference between these DDLs is the individual DDL is identified by individual's name vice position. An ESEP participant does not necessarily assume the position of the engineer or scientist that he or she is replacing.)*

THE INFORMATION CONTAINED IN OR A COPY OF THIS DDL SHALL NOT BE PROVIDED TO THE SUBJECT OF THIS DDL OR ANY OTHER FOREIGN NATIONAL

OFFICE SYMBOL (380-10)

RVA START DATE: 01/01/99

RVA EXPIRATION DATE:01/01/99

DDL APPROVAL NUMBER: 001-99FLO

DDL APPROVAL DATE: 01/01/99

DDL EXPIRATION DATE: *This DDL shall be in effect indefinitely or until the scope is changed, or expire, if it is not a position DDL, upon departure of the foreign representative. Note: RVA expiration date or date indicated in the DAMI-IR approval memorandum.*

SUBJECT: Delegation of Disclosure Authority (DDL) for (IDENTIFY BY POSITION AND COUNTRY), such as TRADOC FLO, DA ASSIGNED NUMBER

1. **CLASSIFICATION:** The highest level of CMI may be disclosed is (INDICATE HIGHEST SECURITY CLASSIFICATION LEVEL AUTHORIZED FOR DISCLOSURE).

2. **DISCLOSURE METHODS:** INDICATE TYPES OF DISCLOSURE METHODS AUTHORIZED. For example: Oral, Visual, and/or Documentary. Documentary means the permanent, physical transfer of CMI to a foreign government. MPEP, ESEP, and CPP participants are limited to "oral and visual" because they do not represent their government. FLOs represent their government and, if authorized in writing by their embassy, may receive CMI authorized for transfer to their government in lieu

Figure E-2. Sample matrix—Continued

of mailing the information to the embassy.

3. **CATEGORIES PERMITTED:** USING CHAPTER 2 OF THIS REGULATION AS A GUIDE, INDICATE THE CATEGORY(IES) OF CMI AUTHORIZED FOR DISCLOSURE.
4. **SCOPE:** INDICATE CLEARLY TO WHOM THE DISCLOSURE AUTHORITY IS GRANTED, FOR WHAT PROGRAM, SYSTEM, STUDY ETC, AND CLEARLY INDICATE THE AUTHORIZED RECIPIENT(S). INDICATE WHAT AGREEMENTS, MOUs, DEAs, FMS CASES, INTERNATIONAL COOPERATIVE PROGRAMS, INSTALLATIONS, AND/OR AGENCIES THAT THE INDIVIDUAL(S) SHALL, IN THE NORMAL COURSE OF DUTIES, DEAL WITH FOR THE DURATION OF HIS TENURE IN THIS POSITION. For example: The Commander, U.S. Army Aviation and Missile Command is delegated authority to disclose CMI within the categories listed in paragraph 3. The Commander may also disclose CMI originated outside of AMCOM when the disclosure is authorized in writing by the originator of the CMI and within the scope of this DDL to the foreign representative assigned to the position listed below:

GOVERNMENT "X" Liaison Officer, _____ Program

Assigned to: U.S. Army AMCOM (THIS IS COMMAND/AGENCY TO WHICH EXTENDED VISIT IS AUTHORIZED)

Associated Installations/Agencies/Commands: White Sands Missile Range, NM; Ft. Bliss, TX; AYX Corporation, New York, NY

THESE ARE ACTIVITIES AND/OR INSTALLATIONS THAT THE INDIVIDUAL SHALL VISIT ON A ROUTINE BASIS AS PART OF ASSIGNED DUTIES AND TO WHICH THE ASSIGNED COMMAND (THROUGH THE CONTACT OFFICER) SHALL ROUTINELY AUTHORIZE VISITS.

Position Description: IN THIS PARAGRAPH, INCLUDE POSITION DESCRIPTION INFORMATION SO THERE IS NO DOUBT AS TO THE DUTIES AND RESPONSIBILITIES OF THE FOREIGN OFFICIAL. BE AS COMPLETE AND AS DESCRIPTIVE AS POSSIBLE TO ENSURE A COMPLETE UNDERSTANDING BY HQDA. INCOMPLETE OR UNCLEAR STATEMENTS CAN RESULT IN UNNECESSARY HQDA STAFFING DELAYS.

5. **AUTHORIZED FOR DISCLOSURE:** IN THIS PARAGRAPH, THE IDENTIFICATION (I.E., CATEGORIES) OF CMI AUTHORIZED FOR DISCLOSURE UNDER THE COGNIZANCE OF THIS DDL MUST BE CLEARLY CITED. IT IS IMPORTANT THAT THE COMMAND OR AGENCY DEVELOPING THE PROPOSED DDL BE DETAILED IN OUTLINING PORTIONS OF

Figure E-2. Sample matrix—Continued

PROGRAMS, SYSTEMS, STUDIES, ETC. THIS PARAGRAPH SHOULD PROVIDE SPECIFIC DETAILS AS TO THE BODY OF CMI THAT THE INDIVIDUAL IS REQUIRED ACCESS IN THE PERFORMANCE OF ASSIGNED DUTIES. TERMINOLOGY USED MUST BE CLEARLY DESCRIPTIVE OF THE CMI TO BE DISCLOSED. THE ANTICIPATED CLASSIFICATION LEVEL SHOULD BE LISTED FOR EACH SPECIFIC TYPE OF INFORMATION. ONCE AGAIN, INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS CAN RESULT HQDA STAFFING DELAYS.

6. **NOT AUTHORIZED FOR DISCLOSURE:** THIS PARAGRAPH MUST SPECIFY THE LIMITS OF THE DISCLOSURE AUTHORITY. THE INFORMATION PROVIDED MUST BE CLEAR AND COMPLETE TO AVOID STAFFING DELAYS. AT A MINIMUM, THE FOLLOWING INFORMATION MUST BE ADDRESSED AND INCLUDED, AS APPROPRIATE:

The following CMI is not authorized for disclosure under the terms of this DDL. Requests for exceptions to these restrictions must be forwarded through foreign disclosure channels to ODCSINT, HQDA.

a. GENERAL:

Intelligence or threat information marked " NOT RELEASABLE TO FOREIGN NATIONALS " (NOFORN).

Restricted Data or Formerly Restricted Data

Information under the cognizance of another Military Department.

Proprietary information owned by a private firm or citizen.

Information obtained from a foreign government.

Data which carries any caveats or markings, which limit access.

Detailed information to include discussions, reports, and studies of system capabilities, vulnerabilities, and limitations which leads to conclusions on specific tactics or other countermeasures, that would otherwise not be assumed and will defeat the system.

Electromagnetic signatures (if applicable to a specific system or portion of a system).

Acoustic signatures (if applicable to a specific system or portion of a system).

Low Observable Requirements or Advanced Signatures Data.

Non-Cooperative Target Recognition Data.

Figure E-2. Sample matrix—Continued

Detailed information related to system hardening against nuclear or directed energy threats.

b. SPECIFIC:

SPECIFIC ITEMS IDENTIFIED AND LISTED AS “*NOT AUTHORIZED FOR DISCLOSURE*” MUST BE INDICATED AT THE SAME LEVEL OF DETAIL AS IN PARAGRAPH 5, ABOVE. INFORMATION THAT IS CLASSIFIED UNDER ORIGINAL CLASSIFICATION AUTHORITY OF AN INDIVIDUAL/AGENCY, OTHER THAN THE DELEGATED AUTHORITY SPECIFIED IN THIS DDL, IS NOT AUTHORIZED FOR DISCLOSURE WITHOUT THE WRITTEN APPROVAL OF THAT INDIVIDUAL/COMMAND/AGENCY. PARAGRAPH 7 PROVIDES PROCEDURES FOR DISCLOSURE OF CMI NOT UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY LISTED IN THIS DDL.

7. PROCEDURES: THE FOLLOWING INFORMATION (AT A MINIMUM) MUST BE INCLUDED IN THIS PARAGRAPH:

The following procedures shall be followed concerning the disclosure or denial of CMI authorized under the terms of this DDL.

a. All CMI disclosure decisions shall be consistent with this DDL, comply with the “Need-to-Know ” principle, and take into account the level of foreign (IDENTIFY) government involvement in the (LIST PROGRAM, STUDY, SYSTEM INVOLVED). CMI disclosure shall be limited to the minimum level of classification and detail necessary to accomplish the specific purpose of the disclosure.

b. APPLICABLE ONLY FOR DOCUMENTATION WHICH MAY BE REQUESTED BY A FLO OR HIS GOVERNMENT. Transfer of classified documents to foreign (IDENTIFY) government representatives shall be processed through government-to-government channels. For the purposes of this DDL, (IDENTIFY) is authorized/not authorized to receipt for CMI identified for disclosure to his or her government.

c. Records of CMI Disclosure Decisions:

(1) Authorized representatives (IDENTIFY BY TITLE SUCH AS CONTACT OFFICER OR POSITION WITHIN THE COMMAND) who disclose CMI (oral, visual, or documentary) to foreign (IDENTIFY) officials SHALL record the disclosure (using DD Form 1822, Report of Disclosure or Denial of U.S. Classified Military Information) and forward the record to the nearest supporting foreign disclosure office, (SPECIFY WHERE DISCLOSURE RECORD IS TO BE FORWARDED, I.E., SECURITY DIVISION, INSTALLATION SUPPORT ACTIVITY, ETC) when one of the following occurs:

(a) First-time disclosures based on one of the following: new information or new (higher) classification level.

Figure E-2. Sample matrix—Continued

(b) The disclosure of information that extends the scope or detail of previously disclosed information.

(c) The authorized disclosing representative shall ensure that all disclosures fitting any of the above categories and the terms of this DDL are reported using the DD Form 1822.

(2) The office responsible for the Foreign Disclosure and Technical Information System (FORDTIS) database shall enter the disclosure decision into the FORDTIS database.

(3) If a FORDTIS terminal is not available, the DD Form 1822 shall be reviewed for completeness by the supporting FDO and forwarded to the next echelon possessing a FORDTIS capability. Instructions for data entry are in DOD 5230.18M, The FORDTIS Users Manual.

d. AUTOMATION:

(1) Access and Use of Computer.

(a) **Access to stand alone computer/NIPRNET:** Foreign representative, Country X is or is not authorized access to stand/alone computer/NIPRNET. **(ISSO/ISSM must provide certification in writing that access is limited to information authorized by the proponent. If authorized e-mail address must include foreign representative's name and country.)**

(b) **Access to SIPRNET/classified systems:** Foreign nationals shall not be permitted access to automated information systems unless the systems have sanitized or configured to ensure that the foreign national's access to CMI is limited to that which has been authorized for release to his/her government. Connectivity to SIPRNET (direct or indirect) requires ODCSINT, HQDA approval PRIOR to granting access, accreditation authority must be notified of this requirement and provide permission in writing for access). ISSO/ISSM must provide certification in writing that the foreign representative can only access CMI information authorized under the terms of this DDL on the system(s) or described within this document.

(i) Standalone computer:

(ii) Network(s): LAN (Describe); WAN (Describe)

(iii) Email: : *(Insert e-mail address and ensure the e-mail address clearly identifies the foreign representative as a foreigner. The recipient of the e-mail must be able to clearly identify the foreign representative as a foreigner.)*

8. U.S. ARMY CONTACT OFFICER: THIS PARAGRAPH MUST INDICATE THE INDIVIDUAL ASSIGNED THE DUTIES OF CONTACT OFFICER FOR THE FOREIGN OFFICIAL. THE CONTACT OFFICER MUST BE ASSIGNED TO THE

Figure E-2. Sample matrix—Continued

SAME COMMAND AND LOCATION AS THE FOREIGN OFFICIAL. THE DUTY ASSIGNMENT, DUTY PHONE NUMBER AND DUTY ADDRESS MUST BE INDICATED IN THIS PARAGRAPH. THIS PARAGRAPH MUST BE AMENDED WHEN A NEW CONTACT OFFICER IS ASSIGNED TO THIS FOREIGN OFFICIAL. AT A MINIMUM, THE DUTIES OF THE CONTACT OFFICER MUST INCLUDE THE FOLLOWING:

- a. Become familiar with the provisions of AR 380-10.
- b. Brief foreign representative regarding DA and local policies and procedures, as well as customs of the U.S. Army.
- c. In conjunction with the FDO, evaluate all requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the approved terms of certification. Consultations and visits beyond the terms of certification require the submission of formal visit requests by the parent foreign government embassy in Washington, DC.
- d. Receive, evaluate, and recommend/refer all requests for CMI to the FDO.
- e. Receive, evaluate, and refer all requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent.
- f. Notify the FDO when the designated contact officer is changed or upon permanent departure of the foreign representative under his or her oversight.
- g. Notify the supporting counterintelligence and local security offices of any foreign visit or activity, which is reportable under the provisions of AR 381-12.
- h. Comply with the procedures regarding misconduct in accordance with AR 380-10.
- i. Brief U.S. personnel with whom the foreign representative shall have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

Figure E-2. Sample matrix—Continued

Delegation of Disclosure Authority Letter for Foreign Participants in FLO, StanRep, MPEP, ESEP, and CPP Positions *(Note: The DDL outlined below is a position DDL and applies to FLOs, StanReps, MPEP, and CPP participants. The DDL for ESEP participants is an individual DDL. The primary difference between these DDLs is the individual DDL is identified by individual's name vice position. An ESEP participant does not necessarily assume the position of the engineer or scientist that he or she is replacing.)*

**THE INFORMATION CONTAINED IN OR A COPY OF THIS DDL
WILL NOT BE PROVIDED TO THE SUBJECT OF THIS DDL OR
ANY OTHER FOREIGN NATIONAL**

OFFICE SYMBOL (380-10)

RVA START DATE: 01/01/99

RVA EXPIRATION DATE:01/01/99

DDL APPROVAL NUMBER: 001-99FLO

DDL APPROVAL DATE: 01/01/99

DDL EXPIRATION DATE: This DDL will be in effect indefinitely or until the scope is changed, or expire, if it is not a position DDL, upon departure of the foreign representative. Note: RVA expiration date or date indicated in the DAMI-IR approval memorandum.

SUBJECT: Delegation of Disclosure Authority (DDL) for (IDENTIFY BY POSITION AND COUNTRY), such as TRADOC FLO, DA ASSIGNED NUMBER

- 1. CLASSIFICATION:** The highest level of CMI may be disclosed is (INDICATE HIGHEST SECURITY CLASSIFICATION LEVEL AUTHORIZED FOR DISCLOSURE).
- 2. DISCLOSURE METHODS:** INDICATE TYPES OF DISCLOSURE METHODS AUTHORIZED. For example: Oral, Visual, and or Documentary. Documentary means the permanent, physical transfer of CMI to a foreign government. MPEP, ESEP, and CPP participants are limited to "oral and visual" because they do not represent their government. FLOs represent their government and, if authorized in writing by their embassy, may receive CMI authorized for transfer to their government in lieu of mailing the information to the embassy.
- 3. CATEGORIES PERMITTED:** USING CHAPTER 2 OF THIS REGULATION AS A GUIDE, INDICATE THE CATEGORY(IES) OF

Figure E-3. Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions

CMI AUTHORIZED FOR DISCLOSURE.

4. **SCOPE:** INDICATE CLEARLY TO WHOM THE DISCLOSURE AUTHORITY IS GRANTED, FOR WHAT PROGRAM, SYSTEM, STUDY ETC, AND CLEARLY INDICATE THE AUTHORIZED RECIPIENT(S). INDICATE WHAT AGREEMENTS, MOUs, DEAs, FMS CASES, INTERNATIONAL COOPERATIVE PROGRAMS, INSTALLATIONS, AND OR AGENCIES THAT THE INDIVIDUAL(S) WILL, IN THE NORMAL COURSE OF DUTIES, DEAL WITH FOR THE DURATION OF HIS TENURE IN THIS POSITION. For example: The Commander, U.S. Army Aviation and Missile Command is delegated authority to disclose CMI within the categories listed in paragraph 3. The Commander may also disclose CMI originated outside of AMCOM when the disclosure is authorized in writing by the originator of the CMI and within the scope of this DDL to the foreign representative assigned to the position listed below:

GOVERNMENT "X" Liaison Officer, _____ Program

Assigned to: U.S. Army AMCOM (THIS IS COMMAND/AGENCY TO WHICH EXTENDED VISIT IS AUTHORIZED)

Associated Installations/Agencies/Commands: White Sands Missile Range, NM; Ft. Bliss, TX; AYX Corporation, New York, NY

THESE ARE ACTIVITIES AND OR INSTALLATIONS THAT THE INDIVIDUAL WILL VISIT ON A ROUTINE BASIS AS PART OF ASSIGNED DUTIES AND TO WHICH THE ASSIGNED COMMAND (THROUGH THE CONTACT OFFICER) WILL ROUTINELY AUTHORIZE VISITS.

Position Description: IN THIS PARAGRAPH, INCLUDE POSITION DESCRIPTION INFORMATION SO THERE IS NO DOUBT AS TO THE DUTIES AND RESPONSIBILITIES OF THE FOREIGN OFFICIAL. BE AS COMPLETE AND AS DESCRIPTIVE AS POSSIBLE TO ENSURE A COMPLETE UNDERSTANDING BY HQDA. INCOMPLETE OR UNCLEAR STATEMENTS CAN RESULT IN UNNECESSARY HQDA STAFFING DELAYS.

5. **AUTHORIZED FOR DISCLOSURE:** IN THIS PARAGRAPH, THE IDENTIFICATION (THAT IS, CATEGORIES) OF CMI AUTHORIZED FOR DISCLOSURE UNDER THE COGNIZANCE OF THIS DDL MUST BE CLEARLY CITED. IT IS IMPORTANT THAT THE COMMAND OR AGENCY DEVELOPING THE PROPOSED DDL BE DETAILED IN OUTLINING PORTIONS OF PROGRAMS, SYSTEMS, STUDIES, ETC. THIS PARAGRAPH SHOULD PROVIDE SPECIFIC DETAILS AS TO THE BODY OF CMI THAT THE INDIVIDUAL IS REQUIRED ACCESS IN THE PERFORMANCE OF ASSIGNED DUTIES. TERMINOLOGY USED MUST BE CLEARLY DESCRIPTIVE OF THE CMI TO BE

Figure E-3. Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued

DISCLOSED. THE ANTICIPATED CLASSIFICATION LEVEL SHOULD BE LISTED FOR EACH SPECIFIC TYPE OF INFORMATION. ONCE AGAIN, INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS CAN RESULT HQDA STAFFING DELAYS.

6. NOT AUTHORIZED FOR DISCLOSURE: THIS PARAGRAPH MUST SPECIFY THE LIMITS OF THE DISCLOSURE AUTHORITY. THE INFORMATION PROVIDED MUST BE CLEAR AND COMPLETE TO AVOID STAFFING DELAYS. AT A MINIMUM, THE FOLLOWING INFORMATION MUST BE ADDRESSED AND INCLUDED, AS APPROPRIATE:

The following CMI is not authorized for disclosure under the terms of this DDL. Requests for exceptions to these restrictions must be forwarded through foreign disclosure channels to ODCSINT, HQDA.

a. GENERAL:

Intelligence or threat information marked " NOT RELEASABLE TO FOREIGN NATIONALS " (NOFORN).

Restricted Data or Formerly Restricted Data

Information under the cognizance of another Military Department.

Proprietary information owned by a private firm or citizen.

Information obtained from a foreign government.

Data which carries any caveats or markings, which limit access.

Detailed information to include discussions, reports, and studies of system capabilities, vulnerabilities, and limitations which leads to conclusions on specific tactics or other countermeasures, that would otherwise not be assumed and will defeat the system.

Electromagnetic signatures (if applicable to a specific system or portion of a system).

Acoustic signatures (if applicable to a specific system or portion of a system).

Low Observable Requirements or Advanced Signatures Data.

Non-Cooperative Target Recognition Data.

Detailed information related to system hardening against nuclear or directed energy threats.

b. SPECIFIC:

Figure E-3. Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued

SPECIFIC ITEMS IDENTIFIED AND LISTED AS “*NOT AUTHORIZED FOR DISCLOSURE*” MUST BE INDICATED AT THE SAME LEVEL OF DETAIL AS IN PARAGRAPH 5, ABOVE. INFORMATION THAT IS CLASSIFIED UNDER ORIGINAL CLASSIFICATION AUTHORITY OF AN INDIVIDUAL/AGENCY, OTHER THAN THE DELEGATED AUTHORITY SPECIFIED IN THIS DDL, IS NOT AUTHORIZED FOR DISCLOSURE WITHOUT THE WRITTEN APPROVAL OF THAT INDIVIDUAL/COMMAND/AGENCY. PARAGRAPH 7 PROVIDES PROCEDURES FOR DISCLOSURE OF CMI NOT UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY LISTED IN THIS DDL.

7. PROCEDURES: THE FOLLOWING INFORMATION (AT A MINIMUM) MUST BE INCLUDED IN THIS PARAGRAPH:

The following procedures will be followed concerning the disclosure or denial of CMI authorized under the terms of this DDL.

- a. All CMI disclosure decisions will be consistent with this DDL, comply with the “Need-to-Know ” principle, and take into account the level of foreign (IDENTIFY) government involvement in the (LIST PROGRAM, STUDY, SYSTEM INVOLVED). CMI disclosure will be limited to the minimum level of classification and detail necessary to accomplish the specific purpose of the disclosure.
- b. APPLICABLE ONLY FOR DOCUMENTATION WHICH MAY BE REQUESTED BY A FLO OR HIS GOVERNMENT. Transfer of classified documents to foreign (IDENTIFY) government representatives will be processed through government-to-government channels. For the purposes of this DDL, (IDENTIFY) is authorized/not authorized to receipt for CMI identified for disclosure to his or her government.
- c. Records of CMI Disclosure Decisions:
 - (1) Authorized representatives (IDENTIFY BY TITLE SUCH AS CONTACT OFFICER OR POSITION WITHIN THE COMMAND) who disclose CMI (oral, visual, or documentary) to foreign (IDENTIFY) officials WILL record the disclosure (using DD Form 1822, Report of Disclosure or Denial of U.S. Classified Military Information) and forward the record to the nearest supporting foreign disclosure office, (SPECIFY WHERE DISCLOSURE RECORD IS TO BE FORWARDED, THAT IS, SECURITY DIVISION, INSTALLATION SUPPORT ACTIVITY, ETC) when one of the following occurs:
 - (a) First-time disclosures based on one of the following-- new information or new (higher) classification level.
 - (b) The disclosure of information that extends the scope or detail of previously disclosed information.

Figure E-3. Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued

(c) The authorized disclosing representative will ensure that all disclosures fitting any of the above categories and the terms of this DDL are reported using the DD Form 1822.

(2) The office responsible for the Foreign Disclosure and Technical Information System (FORDTIS) database will enter the disclosure decision into the FORDTIS database.

(3) If a FORDTIS terminal is not available, the DD Form 1822 will be reviewed for completeness by the supporting FDO and forwarded to the next echelon possessing a FORDTIS capability. Instructions for data entry are in DOD 5230.18M, The FORDTIS Users Manual.

d. AUTOMATION:

(1) Access and Use of Computer.

(a) **Access to stand alone computer/NIPRNET:** Foreign representative, Country X is or is not authorized access to stand/alone computer/NIPRNET. **(ISSO/ISSM must provide certification in writing that access is limited to information authorized by the proponent. If authorized e-mail address must include foreign representative's name and country.)**

(b) **Access to SIPRNET/classified systems:** Foreign nationals will not be permitted access to automated information systems unless the systems have sanitized or configured to ensure that the foreign national's access to CMI is limited to that which has been authorized for release to his/her government. Connectivity to SIPRNET (direct or indirect) requires ODCSINT, HQDA approval PRIOR to granting access, accreditation authority must be notified of this requirement and provide permission in writing for access). ISSO/ISSM must provide certification in writing that the foreign representative can only access CMI information authorized under the terms of this DDL on the system(s) or described within this document.

(i) Standalone computer:

(ii) Network(s): LAN (Describe); WAN (Describe)

(iii) Email: : *(Insert e-mail address and ensure the e-mail address clearly identifies the foreign representative as a foreigner. The recipient of the e-mail must be able to clearly identify the foreign representative as a foreigner.)*

8. U.S. ARMY CONTACT OFFICER: THIS PARAGRAPH MUST INDICATE THE INDIVIDUAL ASSIGNED THE DUTIES OF CONTACT OFFICER FOR THE FOREIGN OFFICIAL. THE CONTACT OFFICER MUST BE ASSIGNED TO THE SAME COMMAND AND LOCATION AS THE FOREIGN OFFICIAL. THE DUTY ASSIGNMENT, DUTY PHONE NUMBER AND DUTY ADDRESS MUST BE INDICATED IN THIS PARAGRAPH. THIS PARAGRAPH MUST BE AMENDED WHEN A NEW CONTACT OFFICER IS ASSIGNED TO THIS FOREIGN OFFICIAL.

Figure E-3. Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued

AT A MINIMUM, THE DUTIES OF THE CONTACT OFFICER MUST INCLUDE THE FOLLOWING--

- a. Become familiar with the provisions of AR 380-10.
- b. Brief foreign representative regarding DA and local policies and procedures, as well as customs of the U.S. Army.
- c. In conjunction with the FDO, evaluate all requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the approved terms of certification. Consultations and visits beyond the terms of certification require the submission of formal visit requests by the parent foreign government embassy in Washington, D.C. .
- d. Receive, evaluate, and recommend/refer all requests for CMI to the FDO.
- e. Receive, evaluate, and refer all requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent.
- f. Notify the FDO when the designated contact officer is changed or upon permanent departure of the foreign representative under his or her oversight.
- g. Notify the supporting counterintelligence and local security offices of any foreign visit or activity, which is reportable under the provisions of AR 381-12.
- h. Comply with the procedures regarding misconduct according to AR 380-10.
- i. Brief U.S. personnel with whom the foreign representative will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

**THE INFORMATION CONTAINED IN OR A COPY OF THIS DDL
WILL NOT BE PROVIDED TO THE SUBJECT OF THIS DDL OR
ANY OTHER FOREIGN NATIONAL**

Figure E-3. Sample format of DDL for foreign participants in FLO, StanRep, MPEP, ESEP, and CPP Positions—Continued

Appendix F Summary Statement of Intent (SSOI)

The SSOI is the counterpart document to the TA/CP and is used in support of international R&D agreements. The format for the SSOI is provided in figure F-1:

The SSOI is the counterpart document to the TA/CP and is used in support of international R&D agreements. The format for the SSOI is provided in figure F-1:

SUMMARY STATEMENT OF INTENT FOR INTERNATIONAL RESEARCH AND DEVELOPMENT AGREEMENT (REVISION 2 - MAY 1995)

1. Header Information:

- a. Short Title of Proposed Project
- b. DOD Proponent
- c. Country/ies Involved

2. Overview of International Agreement

- a. Briefly describe the project. Be specific as to what the project will deliver. Is this a new or existing U.S. project? Is there currently a Memorandum of Understanding or other international agreement in effect that is applicable to this effort?
- b. Is this proposed for Nunn funding? If so, what technological development is to be pursued which is necessary to develop new defense equipment or munitions, or what existing military equipment would be modified to meet U.S. requirements?

3. Operational Requirement

- a. What U.S. operational requirement would this project satisfy and/or what critical deficiency or shortfall would this project address? If known, cite applicable documents.
- b. Briefly describe the project's objectives.
- c. Provide an estimated schedule for the project, and Initial Operational Capability, if applicable.

Figure F-1. Summary statement of intent

4. Partner Nation(s)

- a. Which nations are proposed partners? Which nations have agreed to be partners? What is the assessment (and your basis for it) of foreign interest/commitment?
- b. Briefly describe the proposed negotiation strategy and negotiation schedule.
- c. Describe any planned variations from the policy guidance contained in the latest approved version of the International Agreements Generator, and any resulting variations to the required International Agreement text that are known.

5. Legal Authority. State the statutory legal authority for the proposed agreement. If Arms Export Control Act (AECA), Section 27 is not being used, explain why not.

6. Project Management. Briefly describe how the project will be structured and managed.

7. Benefits/Risks to the U.S. List the advantages and disadvantages of this cooperative project. Address project timing, developmental and life cycle costs, technology to be shared and obtained, impact on U.S. and foreign military capability, and rationalization, standardization and interoperability considerations. Indicate whether there are any risks associated with conducting this project as an international cooperative program, and briefly describe how these risks are to be managed. Is a similar project currently in development or production in the U.S. or an allied nation? If so, could that project satisfy or be modified in scope to satisfy the U.S. requirement?

8. Potential Industrial Base Impact. Briefly describe the potential industrial base impact. Do you anticipate workshare arrangements, requests for offsets, or offshore production of items restricted to procurement in U.S.? Are you aware of any key parts or components with a single source of production? What USG facilities and or contractors would be likely to participate in this cooperative effort? Will there be any significant effects (pro or con) on any U.S. companies or U.S. industrial sector(s)?

9. Funding Availability and Requirements

- a. List the total estimated cost of the International Agreement.
- b. List the cost shares of each participant. Also list the dollar value of any non-financial contributions included in the cost shares.

Figure F-1. Summary statement of intent—Continued

-
- c. If not equitable financially, justify on a program basis (show relative benefit to the Department of Defense). An equitable agreement is defined as one in which a participant's share of contributions to an agreement is commensurate with that participant's share of anticipated benefits from the agreement.
 - d. List the Department's estimated costs by fiscal year, appropriation, and program element. Indicate if these costs have been, or will be, approved in the budget and are available for use.
 - e. List other participants' estimated costs by fiscal year.
 - f. If applicable, outline the likelihood of follow-on research or acquisition and the proponent's commitment to fund such follow-on action.

10. Procurement

- a. Will U.S. DOD participation in the project involve contracting? If so, what agency will perform the contracting, and for what part of the project work?
- b. Will a participant other than DOD perform contracting? If so, which participants and for what part of the project work?
- c. Will contracting be done on a competitive basis? If not, what justification will be used?

11. Information Security and Technology Transfer Issues

- a. Briefly identify the products and/or technologies involved in the program and their NDPC category and classification. The Military Critical Technologies List may be used as a guide.
- b. Is an exception required to the National Disclosure Policy? If so, provide date of approval or date that a request will be submitted to the National Disclosure Policy Committee.
- c. If known, describe the foreign availability of comparable systems and technologies and whether the U.S. technology has been shared through other programs, e.g., FMS, DEA, etc.
- d. Briefly describe the risk of compromise of classified and export controlled technology and/or products and the potential damage to the U.S. military capabilities or technological advantages in the event of such compromise (e.g., negating primary U.S. technological advantage(s), revealing U.S. system weaknesses, development of countermeasures, susceptibility to reverse engineering).

Figure F-1. Summary statement of intent—Continued

-
- e. Identify any measures proposed to minimize the potential risks and/or minimize any damage that might occur due to loss, diversions, or compromise of sensitive classified data or hardware. Specify NDPC categories involved, where applicable. Include any phased release of information designed to ensure that information is disseminated only when and to the extent required to conduct the program; restrictions on release of specific information (including classification, description, and disclosure methods); release of components, software or information in modified form (e.g., export versions, exclusion of design rationale and deletion of data on weapons not sold to the participant); and special security procedures (both government and industrial) to control access to restricted material and information.

12. Proponent's Points of Contact. Include organization, name, telephone, fax, and Internet address. Assure that this POC or an alternate is available to answer any questions from reviewing offices during the RAD review period.

Figure F-1. Summary statement of intent—Continued

Appendix G Frequently Asked Questions

G-1. Concept

The questions cited below are frequently asked of the foreign disclosure community. The corresponding answers reflect the proper responses to these questions.

G-2. Figure G-1 shows frequently asked questions and corresponding answers.

Question: What is proprietary information?

Answer: See chapter 1, paragraph 1-4e(17).

Question: How are DDLs forwarded to ODCSINT, HQDA for review and approval?

Answer: See chapter 2, paragraph 2-10.

Question: Can a FLO develop or assist in the development of the DDL for his or her position?

Answer: See chapter 2, paragraph 2-10.

Question: Under my DDL, can I disclose CMI that was classified by another original classification authority?

Answer: Yes, provided the original classification authority also has a DDL and has authorized the disclosure to you in writing. See chapter 2, paragraph 2-9 for HQDA agency heads and the specific DDLs for MACOM Commanders and MSC Commanders, as applicable.

Question: Can a PEO PM have delegated disclosure authority under a DDL?

Answer: See chapter 2, paragraph 2-10.

Question: How do you identify a foreign representative using a DOD e-mail system to ensure that recipients of his or her e-mail transmissions are aware of his or her status as a foreigner?

Answer: See chapter 3, paragraph 3-5.

Question: Why is recording the first-time disclosures of CMI in the FORDTIS important?

Answer: See chapter 3, paragraph 3-10.

Question: Should DDLs be disseminated outside of FDO channels?

Answer: See appendix E, paragraph E-1f.

Figure G-1. Frequently asked questions and corresponding answers

Question: How do you handle visits of foreign nationals, who are not representing their respective parent government, to U.S. Army commands or agencies?

Answer: See appendix H, paragraph H-5a. Fundamentally, all private citizens, U.S. or foreign national, should be viewed identically as far as visits are concerned. Neither category of individuals has a security clearance and need-to-know, therefore, disclosures of CMI is not an issue. Private citizens, such as foreign national employees and foreign students, who are working under a DA contract shall have access to unclassified information only. CUI may be made available to private citizens working under a DA contract, provided the originator or proponent for the CUI has granted approval and the information is required for the successful completion of the contract.

Question: May DA funds or other resources be used in support of visits by foreign representatives?

Answer: See appendix J, paragraph J-10.

Question: Is a RVA required for a foreign national, who requires access to an Army Installation to perform a service under an U.S. Army contract?

Answer: See appendix J, paragraph J-13.

Question: Can U.S. contractors serve as contact officers?

Answer: See appendix J, paragraph J-14.

Question: What does the command do if a FLO does not sign the certification statement?

Answer: See appendix K, paragraph K-3b(3).

Question: Can a FLO be certified to more than one command or agency?

Answer: See appendix K, paragraph K-3b(1).

Question: When is a RVA required for a FLO to visit U.S. Army or DOD commands or agencies?

Answer: See appendix K, paragraph K-5a.

Question: How will StanReps be handled? Certified to command or agency, or U.S. Army ABCA Office? Visits to other commands or agencies?

Answer: See appendix L, paragraphs L-1 and L-5.

Figure G-1. Frequently asked questions and corresponding answers—Continued

Appendix H Meetings, Conferences and Symposia

Section I Introduction

H-1. Approval policies

AR 380-5 governs the overall Army policy related to the approval of, planning for, and conduct of meetings, conferences, and symposia (hereafter: “meetings”) that are sponsored, co-sponsored, or hosted by U.S. Army agencies or commands. AR 380-10 addresses the foreign disclosure aspects of meetings that involve the attendance or participation of foreign representatives. With the exception of in-house meetings (see definition in glossary), attendance or participation by foreign representatives at many types of meetings—both classified and unclassified—is a possibility that must be considered and planned for. This appendix is intended to supplement overall policies and to prescribe uniform procedures to accommodate and facilitate foreign attendance or participation in meetings, conferences, and symposia, when deemed in the best interests of the Army.

H-2. Types of meetings

For the purposes of this chapter, meetings are divided into two distinct types: those that are acquisition-related and those that are not acquisition-related (see glossary).

Section II Acquisition-Related Meetings

H-3. Rationalization, standardization, and interoperability (RSI)

RSI considerations and bilateral agreements promoting industrial cooperation have resulted in DA’s adoption of policies (AR 34-1) that effectively expand foreign attendance and participation at meetings. These policies require that—

a. Qualified government and industry representatives from U.S. allies and other friendly nations with which DOD has entered into reciprocal procurement agreements are to be afforded opportunities to compete on a fair and equitable basis with U.S. industry for DOD acquisition contracts—subject to U.S. laws and regulations.

b. Representatives are afforded suitable access to technical information necessary for such competition. Therefore, attendance by foreign representatives must be planned for at any meeting at which U.S. industry is represented. The most prevalent acquisition-related meetings are—

(1) Scientific and technical meetings convened under AR 70-26.

(2) Advance planning briefings for industry convened under AR 70-35.

(3) Meetings convened in cooperation with private, industrial-related associations (for example, Association of the U.S. Army, American Defense Preparedness Association, National Security Industrial Association, Armed Forces Communications and Electronics Association).

H-4. Planning

Acquisition-related meetings are distinct from other types of meetings in several ways that tend to complicate planning and require special procedures. The requirement to consider foreign industrial participation in Army contracts will require early consideration of foreign disclosure issues. The procuring contracting officer (PCO) is responsible for obtaining an Army position on foreign participation. This position must determine which foreign nations may be eligible to receive the information to be disclosed by the contract. Successful foreign participation in cooperative developmental contracts, either as a prime or subcontractor, may require the disclosure of CMI. Therefore, Army PMs or item managers must involve their FDO in the process prior to advertising in the Commerce Business Daily (CBD) and must consider such issues as—

a. The advisability of including foreign contractors in the project.

b. The time and costs that must be built into a contract to allow for the approval process for munitions licensing. Documentary transfer of classified deliverables (for example, interim reports, final reports) from U.S. contractor team members to foreign participants can be a lengthy process. If not considered prior to award of a contract, DOD review requirements may consume an inordinate amount of time when work under the contract begins.

c. The maximum eligibility level for classified material in each NDP-1 category that may be involved. It is essential to remember that requests for information (RFIs) and requests for proposals (RFPs) are merely tools in the contract process. A contract potentially involving classified information may only require an UNCLASSIFIED RFI or RFP.

Nonetheless, only foreign nations for which disclosure authority has been delegated to the Army under NDP-1 for the categories of CMI involved may be considered for participation in the contract.

d. The benefits or liabilities in having foreign industrial participation versus the sensitivities of CMI involved in the project must be weighed.

H-5. Procedures

After making a preliminary determination to convene or sponsor an acquisition-related meeting that may involve foreign representatives, an Army command or agency is to adhere to the following procedures, based on the sensitivity of the information to be disclosed.

a. Unclassified meeting open to the public. ODCSINT, HQDA approval to convene an unclassified meeting open to the public is not required.

(1) Commanders may exercise their delegated visit authority to approve this type of meeting (see appendix J).

(2) The U.S. sponsor will notify all participants that presentations must be approved for disclosure to the public. Criteria for approval and procedures for obtaining such approval are contained in AR 70-31 and AR 360-5. DOD 5220.22-M governs presentations by contractor personnel when the information in question is derived from or acquired as a result of a DOD contract. The ITAR or Department of Commerce EAR, as applicable, governs presentations by non-USG personnel when the information in question is not derived from a DOD contract.

(3) The U.S. sponsor and presenters participating at any unclassified public meeting should be aware that technical documents resulting from contracted fundamental research efforts will normally be releasable to the public, except in those rare and exceptional circumstances where there is a high likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to defense, and agreement on this situation has been recorded in the contract or grant.

b. Unclassified meeting closed to the public. ODCSINT, HQDA approval to convene an unclassified meeting closed to the public is not required.

(1) Attendance of foreign representatives must be requested in the manner prescribed in appendix J of this regulation. Note: Canadian citizens may be certified by the Joint Certification Office (JCO), according to AR 70-31 and subject to ITAR limitations.

(2) Coordination will be effected with all DA agencies or commands having a proponent or other substantive interest in the subject matter of the meeting to establish attendance criteria for foreign representatives prior to publicizing the meeting. In this regard, it is important to consider the prohibition on false impressions in paragraph 2-2 of this regulation.

c. Classified meetings. Meetings involving the disclosure of CMI to foreign representatives require the designation of a security sponsor and approval by ODCSINT, HQDA. This approval is to be obtained in the manner prescribed in AR 380-5, chapter 6.

(1) Attendance of foreign representatives must be requested in the manner prescribed in appendix J of this regulation.

(2) Approval for the disclosure of CMI will be according to this regulation.

Section III

Non Acquisition-Related Meetings

H-6. Unclassified meetings

a. Cooperative development meetings involving only unclassified information do not require prior approval of ODCSINT, HQDA; however, attendance of foreign representatives must be requested in the manner prescribed in appendix J of this regulation.

b. Coordination will be effected with all DA agencies or commands having a proponent or other substantive interest in the subject matter of the meeting to establish attendance criteria for foreign representatives prior to publicizing the meeting. In this regard, it is important to consider the prohibition on false impressions in paragraph 2-2 of this regulation.

H-7. Classified meetings

Meetings involving the disclosure of CMI to foreign representatives require the designation of a security sponsor and approval by ODCSINT, HQDA. This approval is to be obtained in the manner prescribed in AR 380-5, Chapter 6.

a. Attendance of foreign representatives must be requested in the manner prescribed in appendix J of this regulation.

- b.* Approval for the disclosure of CMI will be according to this regulation.

Appendix I Policy and Procedures for Disclosure of CMI in Support of International Activities

Section I Introduction

I-1. Concept.

Overall policies and procedures governing DA participation in international activities stemming from international agreements are contained in various Army regulations—principally in the 12, 34, and 70 series.

I-2.

The policies and procedures regarding foreign involvement in the materiel acquisition process is more complicated and warrants additional guidance (Also see appendices C through F, and H).

Section II Security Assistance/DCS-Related Disclosures of CMI

I-3. Policy

a. This section will cover and guide the disclosure of CMI in cases involving the transfer of defense articles or services (including training). This transfer is conducted either on a government-to-government basis or on a licensed, DCS basis. Transfer means the sale, lease or loan, grant, co-production, or reciprocal use. The transfer must be accomplished per agreements created under the provisions of AR 12-1, AR 12-8, or ITAR.

b. When a transfer involves the proposed disclosure of CMI, agreements leading to the transfer must be coordinated and approved as prescribed in chapter 2 of this regulation. Such agreements principally involve the disclosure of information in Categories 2, 4, and 8. In all cases where there is neither an Army export policy nor system DDL, potential security assistance Letter of Offer and Acceptance (LOA) involving the disclosure of CMI in conjunction with or as a result of the first-time sale of a major end item (including components, armaments, ordnance, etc.) will be coordinated with ODUSA(IA) and ODCSINT, HQDA, prior to final approval of the LOA.

c. Technical information proposed for transfer to a foreign government or international organization must be carefully reviewed to exclude any design, manufacturing, production, or system integration technology that has not been specifically approved for foreign disclosure and subsequent transfer under the system DDL.

d. In keeping with NDP-1, the transfer of a single materiel item to a foreign government or international organization is normally prohibited. An exception may be made under certain conditions, such as if the prospective recipient would reasonably require no more than one in its inventory. An exception for leases or loans for the purpose of test and evaluation is discussed in paragraph I-6.

e. In a security assistance context, the coordination process is also referred to as determining willingness to sell. It may be the result of a foreign government's request for price and availability (P&A) data submitted through channels as prescribed in AR 12-1. It may also be initiated unilaterally by DA or DOD in anticipation of potential sales or transfers as a result of a foreign government's request or a license application through the Department of State (required for a DCS).

I-4. Disclosure of CMI in security assistance initiatives

a. Disclosures Pending Decision of U.S. Willingness to Sell. Pending HQDA determination of willingness to sell or otherwise transfer materiel to a specific foreign government or international organizations, no CMI (irrespective of category) related to the materiel may be approved for disclosure.

b. Disclosures after a decision not to sell. If HQDA decides against the sale or transfer of materiel, disclosure of information to the particular foreign government or international organization will be limited to that releasable to the public. For example, public domain information on a specific weapons system may be disclosed in the context of a domestic U.S. Army capability briefing.

c. Disclosures after a decision to sell. If HQDA decides to sell or transfer classified materiel, disclosure will be according to chapter 2 of this regulation. General guidance is as follows—

(1) Provided all NDP-1 conditions have been satisfied and prior to formal acceptance of the LOA by the foreign recipient, disclosure is usually limited to the CONFIDENTIAL level. This information may include P&A data, information on general system characteristics and capabilities, and system-related training information necessary to successful operation and maintenance. Specific information on system countermeasures susceptibilities or vulnerabilities or countermeasures capabilities may not be considered for disclosure until the sale is consummated, and then only on a case-by-case basis.

(a) The information specified in paragraph I-4c(1) is deemed essential and sufficient for a foreign government to make an informed judgement regarding potential acquisition or purchase decision. It may be exceeded only on approval by DUSA(IA), after coordination with ODCSINT, HQDA for compliance with NDP-1 and issuance of additional disclosure authority.

(b) CMI approved for disclosure, but disclosed in any manner other than with issuance of a LOA or letter of instruction, will be accompanied by the stipulation that the disclosure is not to be construed as a USG commitment to sell or transfer the materiel or provide further related information.

(2) After a foreign recipient has formally accepted a LOA, disclosures may be approved to the limits of the Army's delegated disclosure authority for the country according to NDP-1 (to include all restrictions), and existing Army export policy and system DDL. The CMI disclosure must be directly related to the designated item approved for sale.

d. Special considerations. Prior to making a commitment to sell, proposed disclosures of other categories of CMI relating to the sale or transfer of U.S.-produced end items through security assistance channels will be governed as follows—

(1) Special consideration must be given to possible intelligence, security and special technology information implications. For example, separate authorization, as identified in NDP-1, must be obtained for the disclosure of COMSEC, cryptographic information, intelligence threat data, low observable, and non-cooperative target recognition, etc. Authorization to disclose these types of information must be obtained prior to rendering a final decision on the transfer of the end item to a foreign government or international organization.

(2) Disclosure of classified production information is prohibited without the approval of ODCSINT, HQDA.

I-5. Disclosure of CMI on a licensed commercial basis

a. Mutual security assistance interests of the U.S. and foreign governments may at times be served better by the transfer of defense articles or services on a DCS basis. All initiatives involving defense articles and services are subject to munitions licensing prescribed by the Department of State ITAR, which implements the AECA. ODUSA(IA) is the HQDA proponent responsible for the review of licenses for the export of defense articles and services, and USASAC is the Executive Agent for the execution of the Munitions Licensing Program. Overall DA policies and procedures governing the processing of munitions license applications are contained in AR 12-8.

(1) In coordination with ODUSA(IA), ODCSINT, HQDA will review selected munitions license applications referred to the Army by the Department of State and OSD to ensure Army compliance with foreign disclosure policies.

(2) DA command or agency FDOs will review all munitions license applications forwarded to their respective commands or agencies to ensure foreign disclosure policy compliance. DA command or agency FDOs will use DA Form 4605-R (Department of the Army Munitions Control Case Processing Worksheet) in their review of all munitions licenses. Additionally, the FDO will consider the disclosure criteria cited in figure 2-1. In this regard, the commercial sale of a major, classified U.S. Army weapon system, the PM, with assistance from the supporting FDO, for that weapon system will be responsible for overseeing the commercial sales case and ensuring U.S. contractor compliance with current U.S. Army and USG export and disclosure policy provisions. The PM will report any conflict with established export policies to ODUSA (IA), ODCSINT, HQDA, and USASAC.

b. Data regarding the status of and substantive details regarding munitions license applications processed by DA and DOD are reflected in the FORDTIS.

I-6. Foreign test and evaluation of materiel

Administrative and operational requirements and restrictions governing the foreign test and evaluation of U.S. materiel are prescribed as follows:

a. Foreign test and evaluation of DA classified equipment may be authorized for disclosure when the tests—

(1) Are on an item approved for foreign disclosure by the appropriate disclosure authority.

(2) Can be performed at a DA installation or under other strict DA control that guarantees appropriate safeguards for classified information and classified critical technology.

b. Exceptions to paragraph I-6a(2), such as the transfer of single classified military items for test and evaluation under foreign security control, may be authorized only when all of the following conditions are satisfied:

(1) There is no transfer of technology that the U.S. would not license for manufacture in the foreign country.

(2) There is no transfer of equipment that would not be approved for foreign sale or export to the foreign country, if requested.

(3) The transfer will result in a clearly defined advantage to the DA and the USG. Examples are outlined below:

(a) Avoidance of significant costs and or acceleration of developmental programs with U.S. allies.

(b) Advancement of standardization objectives with U.S. allies.

(c) Exchange of technical and scientific information of common interest on a mutually beneficial basis.

(4) Proposals to authorize foreign test and evaluation in this manner, including reciprocal use loans of materiel under AECA, Section 65, will be submitted to ODUSA(IA), which will—

- (a) Coordinate with counterpart elements of the Air Force and Navy, depending on their interest in items or technologies associated with the information proposed for transfer.
- (b) Coordinate with the OASA(ALT), ODCSINT, and other HQDA staff agencies having an interest in the issue.
- (c) On coordination and concurrence of all concerned, staff the issue with the Under Secretary of Defense for Acquisition and Technology.
- (d) Provide to ODCSINT, HQDA a copy of the proposal. ODCSINT, HQDA will notify the NDPC Secretariat, as necessary.
- (5) The Secretary of the Army, in coordination with the Office of the Under Secretary of Defense for Acquisition and Technology, approves the exception as satisfying the above criteria.
- (6) The test is performed pursuant to a test and evaluation agreement, lease arrangement, or sales contract containing requisite security controls.
- (7) Documentary CMI will be disclosed under this program only after both parties have approved the test program.

I-7. Disclosure of CMI in security assistance-related training

Training of foreign representatives at DA activities or at U.S. contractor facilities under DA sponsorship is to be according to AR 12-1, AR 12-8, and AR 12-15. See appendix J for information regarding the conduct of orientation tours and visits, and AR 12-15 for information concerning the exchange of units for training.

a. DA CMI contained in training courses or otherwise to be presented to foreign trainees are to be approved for disclosure pursuant to this regulation. To preclude potential false impressions, disclosure determinations must be made for specific countries before the course is placed on the Military Articles and Services List or otherwise indicated as available for foreign attendance.

b. A foreign trainee may receive training on U.S. equipment that is classified or involves classified information, provided the equipment is in the inventory of the trainee's government or an international agreement/purchase agreement has been concluded with the USG to acquire the equipment and training. CMI disclosed during training will be limited to the specific version of the equipment purchased or committed to purchase and subject to any other condition related to that particular version of the equipment. The PM or materiel developer will be responsible for notifying U.S. Army TRADOC of the specific configuration of a weapon system purchased by a foreign government or international organization and providing disclosure guidelines, particularly conditions and limitations related to that specific configuration and the foreign recipient. U.S. Army TRADOC has primary responsibility for ensuring that the program of instruction for the training of foreign trainees complies with all disclosure conditions.

c. The inclusion of foreign trainees from more than one foreign government should be avoided when the CMI to be disclosed varies due to the different versions of the same equipment purchased by the individual foreign governments. If this situation cannot be avoided, the specific CMI will be equally suitable for disclosure to all foreign participants, unless authority is obtained to disclose CMI beyond that which has already been authorized disclosure to a particular or group of foreign governments.

d. At the discretion of DA agencies and commands conducting or supervising training, course-related classified documentary material (such as, DA and school publications, student notes) may be authorized for retention by foreign trainees. Such materials must be transmitted to the foreign trainees through U.S. security assistance officials located in the trainees' home country.

e. Foreign trainees may participate in, or conduct training on, third-country equipment only with the written consent of the government that provided the equipment.

Section III

Research and Development (R&D) Materiel-Related Disclosure of CMI

I-8. Concept

a. This section pertains to the disclosure of CMI in Category 3. Such disclosure occurs when cooperative R&D efforts are undertaken with allied and other friendly governments and international organizations.

b. International cooperative R&D efforts may be categorized by subject matter, for example—

- (1) NATO or ABCA RSI (AR 34-1).
- (2) International Cooperative R&D (AR 70-41).
- (3) The Technical Cooperation Program (TTCP) (AR 70-23).
- (4) Mutual Weapons Development Data Exchange Program (MWDDEP) and DDEP (AR 70-33).
- (5) U.S.-Canada Defense Development Sharing Program (AR 70-66).
- (6) Specific agreements covering one or more designated subjects (such as, international participation in Army proponent programs covered by Ballistic Missile Defense Organization (BMDO)).

c. Excluded are agreements regarding the ESEP (AR 70-58) and MPEP (AR 614-10).

I-9. Disclosure in Support of International Cooperative R&D Agreements

a. Proposed international cooperative R&D efforts involving the disclosure of CMI must be processed under AR 70-

41, AR 550-51, and this regulation. Once approved, the existence of an agreement neither obligates approval nor constitutes advance approval of the disclosure of any specific CMI. Such an agreement forms the basis for disclosure consideration only. The U.S. proponent will be responsible for ensuring that a reasonable and balanced quid-pro-quo is achieved and maintained.

b. Each international cooperative R&D agreement is to contain mutually-agreed parameters for information exchange. Additionally, each agreement is to be supported by a SSOI and DDL (if disclosure of CMI is involved). The DDL, approved by ODCSINT, HQDA, will accompany the SSOI during the staffing process.

c. Except for co-development agreements, CMI considered for disclosure within the scope of international cooperative R&D agreements is usually limited to Category 3 technology base information, Budget Activities 1 through 3 (see glossary). The disclosure of system-specific developmental CMI under other types of R&D cooperative agreements (such as DEAs or IEAs), and TRDP and Advanced Cooperative Technology Development (ACTD) MOUs) will be considered on a case-by-case basis. Such disclosures will require the concurrence of the ODCSINT, HQDA, ODUSA(IA), and the system developer.

I-10. CMI disclosures involving materiel changes and improvements

Routine CMI disclosures involving materiel changes and improvements (that is, modification work order (MWO), engineering change proposal (ECP), or PIP) will be according to the system TA/CP and DDL. Changes or improvements which, if incorporated, would significantly improve performance, decrease vulnerability to countermeasures, or otherwise constitute new classified information, must be approved by ODCSINT, HQDA for disclosure prior to any commitment to international participation. For example, improvements that would require a new designation for an end item such as the comparison of the AH-64A Apache and the AH-64D (Longbow) helicopters. Proposals are to be referred to HQDA in the same manner prescribed in chapter 2 of this regulation. A separate ENDP approval may be necessary to permit disclosure of CMI related to MWO, ECP, or PIP to any foreign government for which the initial item or system acquisition required an ENDP request.

I-11. CMI Disclosure to Foreign Exchange and Cooperative Program personnel participating in DA R&D activities

DA policies and procedures governing the certification of foreign personnel into the DA work force are contained in appendices M through O. Exchange and Cooperative Program Personnel participating in DA R&D activities will only be assigned to DA pursuant to an appropriate international agreement. Foreign personnel will not be assigned to duties that will require access to DA CMI beyond that which is authorized for disclosure to his or her parent government..

I-12. Foreign participation in classified acquisition contracts

See appendix H.

Appendix J DA International Visits Program

Section I General

J-1. Concept

The DA International Visits Program has been established to ensure that CMI to be disclosed to foreign visitors has been properly authorized for disclosure to their governments and that the requesting foreign government provides security assurances for such visitors. Additionally, the DA International Visits Program serves to facilitate administrative requirements for the visit.

J-2. Control of visitors

Visits by foreign representatives to DA activities and DA contractor facilities will be controlled to ensure that the visitors receive access to only that CMI authorized for disclosure to their government by a disclosure official designated according to this regulation. CMI will not be disclosed to a foreign representative unless the appropriate Disclosure Authority has received security assurances from that person's government. In all cases, AR 190-13 and local security policies and procedures will apply for the control of foreign representative visitors in restricted access areas, such as badges and escorts.

J-3. Informal coordination

The fact that a proposed visit begins by informal coordination does not eliminate the need for an official visit request and authorization. This requirement must be clearly understood by all affected parties to avoid mutual confusion and embarrassment. Only an accredited foreign military attaché may propose and request visits by his or her country's

representatives. These proposals and requests become official only upon the presentation of a RVA to ODCSINT, HQDA by appropriate foreign attaché personnel. While informal contacts with foreign representatives may often lead to the submission of a RVA, DA officials must remember that commitments made during these informal contacts are not binding on ODCSINT, HQDA.

J-4. CMI documentary transfers

See chapter 3, Section I of this regulation for detailed information. Note: This section applies to documentary transfers of CMI only. Transfers of CUI will be at the discretion of the originator or proponent according to the appropriate regulation.

J-5. Foreign Visits System (FVS) requirements

Foreign government RVAs will be submitted by the accredited military attaché or designees using the FVS. Requests for visits by governments that do not participate in the FVS will be submitted by the accredited military attaché, in writing, directly to ODCSINT, HQDA, which will enter and process the request in the FVS.

J-6. Visit requests from countries without a military attaché

If a foreign government does not have a military attaché diplomatically accredited to the U.S., a foreign government embassy official or the senior U.S. military representative located in the prospective visitors' parent country may prepare and submit the RVA to ODCSINT, HQDA for consideration. The RVA must conform to the policies and procedures for submission of RVAs in this regulation and DODD 5230.20.

J-7. Invitations

While the majority of foreign representative visits are initiated by foreign governments, DA officials may extend invitations to foreign representatives.

a. Formal invitation. In instances where it is desirable to expend representational (speakers, participants in research projects, and the like) or security assistance, or International Military Education and Training (IMET) funds to invite foreign nationals or representatives to visit military facilities under Army sponsorship, the DA host will do so according to Army regulations governing such funding. All such visitors will travel on ITOs or honorariums (RVA not required) published by competent authority.

b. Informal invitation. DA agencies and commands extending informal invitations to foreign representatives, without expenditure of U.S. funds, must ensure that the invitation states the invitees or their government must defray all costs associated with the visit and a RVA must be submitted through the foreign government's embassy according to the self-invited visit procedures identified in this appendix. Before issuing the informal invitation, DA officials will inform the appropriate FDO of the proposed issuance of the invitation and the extent of any anticipated disclosure of CMI to ensure compliance with this regulation.

J-8. Standards of appearance

All foreign military visitors (to include accredited military attachés, assistant military attachés, exchange personnel, and liaison officers) are expected to wear their respective country's uniform unless directed otherwise by an appropriate DA authority. If required by local policy, a clearly identifiable badge should be provided to the foreign representative to wear, identifying him or her as a foreign representative.

J-9. Out of channel visit requests

RVAs sent directly to DA commands or agencies by other USG departments or agencies, nonmilitary international organizations in which the USG maintains membership (such as the United Nations), or foreign governments—will be immediately referred to ODCSINT, HQDA for action, unless delegated visit authority has been granted.

J-10. Funding and other support rendered to foreign representatives

No DA funds or other resources may be used to support the activities of foreign representatives while visiting or certified to DA, except when authorized by and consistent with applicable U.S. law, and DOD and U.S. Army guidance.

Section II

Self-Invited Visit Procedures

J-11. Requests for self-invited visit authorizations

a. One-time visit authorizations. One-time visit authorizations will be used to permit contact by foreign representatives with a DA element or a DA contractor facility for a single, short-term occasion (fewer than 30 days) and for a specified purpose. Authorizations expire on the end of visit date, unless extended by an amendment. Within 72 hours of the approval of the request, visitors will arrange visit details directly with the facility to be visited.

b. Recurring visit authorizations. Recurring visit authorizations permit separate visits over a specified period of time

(normally 1 year) in connection with a government-approved license, contract, agreement, or other programs. Authorizations will be valid for the duration of the program, subject to annual review, revalidation, and the specific requirements of the U.S. Army.

c. Extended visit authorizations (EVAs). EVAs will be used to permit a single visit for an extended period of time, normally beyond 30 days. The authorization will be valid for the duration of the program, assignment, or certification, subject to annual review and revalidation. EVAs will be used in the following situations:

- (1) Certification of a FLO, foreign exchange personnel (ESEP and MPEP), or CPP to a DA activity.
- (2) Training at a contractor facility under an FMS case, except for those individuals on ITOs. If it is in the U.S. Army's interest, Army-sponsored training at a contractor or Army facility under DCS.
- (3) Assignment of a foreign contractor's employee if the foreign contractor is under DA contract, and performance on the contract requires assignment of the employee to the Army or Army element at a contractor facility. This individual will be considered a FLO.

d. Submission of self-invited RVAs. In all of the above self-invited visits, ODCSINT, HQDA approval is required prior to any formal visit to a DA activity or facility. RVAs for self-invited visits must be submitted 30 days prior to the proposed commencement date of the visit. The only exception to the 30-day rule involves the U.S. Army National Training Center and EVAs for certification of foreign representatives, which require RVAs 45 days in advance of the proposed visit date. These requirements are outlined in a handbook issued by ODUSA(IA) to each embassy that has a military attaché accredited to the U.S. Army. All amendments to approved RVAs must be accepted by the hosting command or agency prior to becoming effective. Hosting commands or agencies will notify ODCSINT, HQDA of any violation of this provision. Unannounced or unscheduled visits to DA facilities where foreign representatives arrive at an Army activity or facility without prior notice or official approval will not be permitted to proceed. In those instances, the Army command or agency will immediately report the incident to ODCSINT, HQDA, which will provide instructions to the Army command or agency and notify the parent government's military attaché of the violation. Additionally, ODCSINT, HQDA will then coordinate with the Director of Foreign Liaison, ODUSA(IA) to determine whether further action is necessary.

J-12. Assignment, evaluation, and processing of RVAs

a. Initial RVA review. Upon receipt in ODCSINT, HQDA, the RVA will be screened to determine compliance with basic administrative requirements, and accepted for further processing (see Figure J-1), or rejected.

- (1) If rejected, the RVA is returned with annotations reflecting the rationale for the rejection.
- (2) If accepted, the RVA is assigned for action and information to the appropriate Army addressees on the following basis:

(a) A RVA to an Army location is assigned for action to the DA agency or MACOM exercising jurisdiction over the information, organization or activity to be visited. The RVA is assigned for information to the organization to be visited (if other than the action addressee), all intermediate headquarters, and all Army addressees having an interest in the subject matter of the visit.

(b) A RVA to a defense contractor is assigned for action to the appropriate U.S. Army acquisition authority and for information to addressees having an interest in the subject matter proposed for discussion.

(c) Staffing of RVAs by ODCSINT, HQDA, is without prejudice; that is, staffing indicates only that DA has administratively accepted the RVA for processing and is not to be construed as HQDA's solicitation of concurrence, nor predisposition towards approval.

b. RVA evaluation (administrative factors). In evaluating a RVA, the command or agency will apply the administrative factors below. If the response to any of the first three factors is negative, the command or agency must recommend that the RVA be returned to the requestor without action.

- (1) Is the expressed purpose of the proposed visit understandable and sufficiently detailed to permit due consideration from a substantive perspective?
- (2) Is the proposed visit date sufficiently in the future to permit necessary preparation for the visit and required coordination for disclosure determinations? Is the proposed visit date acceptable to the prospective host?
- (3) Is sufficient justification for the visit and associated discussions included in the RVA to permit disclosure determinations?
- (4) Is sufficient rationale presented in the RVA—or known to the action addressee or prospective host—to justify intermittent, repetitive visits, if so requested?

c. RVA evaluation (substantive factors). In evaluating a RVA, the following substantive factors must be considered:

- (1) If the RVA is administratively acceptable, the RVA action addressee or prospective host must determine whether—from its perspective—the best interests of the U.S. Army would be served in approving the visit. Evaluators should bear in mind that visits almost always involve the disclosure of official Army information that is for internal Army use only (that is, not in the public domain) and, in some cases, CMI. In either case, disclosures to foreign representatives require that a valid requirement for the information (need-to-know) exists and that such disclosures would result in a net benefit to DA and DOD. Thus, resolving information disclosure-related issues is essential and prerequisite to a determination of whether the best interests of the U.S. Army would be served in approving the visit.

Note: Should the RVA action addressee or prospective host desire political-military advice regarding the requested visit, it should contact ODUSA(IA), HQDA.

(2) Need-to-know and net benefit should be considered in the context of DA participation in international activities related to the proposed visit. However, it is imperative that such participation not obligate DA to disclose CMI. Instead, each potential disclosure of CMI must be considered on its own merits and be based on an affirmative response to the question: "Is the disclosure essential to achieve the stated purpose of the visit?" If not, the action addressee or prospective host must recommend denial or hosting the visit at the unclassified level.

(3) If the above substantive factors are satisfied, it is then necessary to establish specific, substantive disclosure parameters for discussions during the visit. Evaluators are to be guided in this regard by the following factors:

(a) What substantive category or categories of information are involved?

(b) What is the minimum classification level of the information that must be disclosed to accomplish each aspect of the purpose of the visit and has there been prior disclosures of that CMI?

(c) Given the category of information involved and the minimum classification level necessary for meaningful discussions, how is disclosure determined?

1. CMI is within the substantive scope of an existing international activity and its associated DDL (program or organization).

2. CMI that is not within the authority of a DDL requires approval by ODCSINT, HQDA. Such a proposal constitutes a new or a modification to an existing disclosure program and must be accompanied by complete justification or a request for a one-time disclosure exception. If a proposal requires an exception to NDP-1, the visit will not be approved at that time. If the command or agency to be visited deems that the U.S. Army should sponsor an ENDP request for a future visit or interaction, the command or agency will comply with procedures cited in appendix C.

3. Criteria for evaluating an RVA to a DA contractor facility. Army-sponsored visits by foreign representatives to DA contractor facilities constitute exemptions to the licensing requirements of the ITAR and the EAR. These visits will involve the disclosure of U.S. Army information in support of actual or planned international programs (that is, FMS, cooperative R&D, etc.). DA-sponsored visits will not be used to circumvent the licensing requirements of the ITAR (that is, DA contractor's independent marketing efforts).

d. MACOM recommendation. The MACOM will recommend to ODCSINT, HQDA:

(1) Visits to DA command or agency.

(a) Approval of the visit request and provide disclosure guidance if it is in support of an actual or planned DA program (include the name and commercial duty telephone number of the contact officer and point of contact, if not the same person; DDL number, international or functional agreement, advance coordination instructions for recurring RVAs, etc.); or,

(b) Denial of the visit request if it is determined that the information associated with the proposed visit cannot be authorized for disclosure (include basis of rationale, that is, beyond scope of established international agreement, conflicts with NDP-1, etc.).

(2) Visits to DA contractor facility.

(a) Approval of the visit request (this approval converts the visit into a sponsored visit) and provide disclosure guidance if it is in support of an actual or planned DA program (include the name and commercial duty telephone number of the contact officer and point of contact, if not the same person; DDL number, international or functional agreement, advance coordination instructions for recurring RVAs, etc.); or,

(b) Denial of the visit request if the visit is not in support of an actual or planned USG program or if it is determined that the information associated with the proposed visit cannot be authorized for disclosure (include rationale).

e. Army decision. Upon receipt of the recommendation of approval or denial, ODCSINT, HQDA will on behalf of HQDA, officially respond to the RVA (approval or denial).

(1) RVA denial. If the RVA is denied, notify the requester, affected Army elements, and DA contractors, as required, of the decision. Note: Denial of the RVA does not preclude the requester or the affected DA contractor from making direct arrangements according to ITAR provisions.

(2) RVA approval. If the RVA is approved, notify the requester, affected Army elements, and DA contractors, as required, of the decision.

(a) Issue any instructions, limitations, etc. as well as the name and commercial duty telephone number of the U.S. Army contact officer.

(b) Notify requesting military attaché that he or she or the prospective visitor must initiate contact and resolve administrative details with the host. Arrangements must be confirmed 72 hours after RVA approval. An earlier deadline may be specified by the prospective host in its response to ODCSINT, HQDA.

Section III

Delegation of Visit Authority

J-13. Delegation of visit authority to approve certain visits by foreign representatives

Under certain circumstances as described below, the DCSINT, HQDA may delegate authority to specified heads of HQDA agencies and MACOM commanders to approve visits by foreign representatives to organizations, agencies, activities, installations, and facilities under their jurisdiction. Such visits must be consistent with OPSEC practices (AR 530-1) and local security procedures. All disclosures of CMI in conjunction with any delegation of visit authority will be according to a DDL, or equivalent disclosure authorization document. The agency head or MACOM commander may further delegate this visit approval authority to organizations, agencies, activities, installations, and facilities commanders under his or her cognizance. Note: To assist commanders or agency heads, this paragraph also addresses the potential visits of foreign nationals, who are not representing their respective government, to U.S. Army commands and agencies. The approval authority for these types of visits is vested in the commander or agency head.

a. Authority is delegated to approve—

(1) Visits to participate in social activities (irrespective of agency or command sponsorship or involvement), activities open to the general public (such as Armed Forces Day open house), international sporting events, or official activities to which members of the public have been invited (such as a wreath-laying ceremony). Such visits will involve the disclosure of public domain information only.

(2) Visits to obtain authorized routine or emergency medical treatment. Such visits will involve the disclosure of public domain information only.

(3) Transient visits (such as brief stopovers on a flight). Such visits will involve the disclosure of public domain information only.

(4) Visits in the performance of an unclassified Army contract or scientific/R&D agreements with U.S. academic or research institutions. This includes visits in the performance of an unclassified contract or scientific/R&D agreement sponsored by another DOD component or Federal agency.

(5) Visits by foreign representatives sponsored by another DOD or Federal agency. Such visits may involve the disclosure of CMI. Visits by foreign nationals sponsored by another DOD or Federal agency will only involve unclassified information.

(6) Visits by foreign military students under ITOs as a part of an FMS case. Such visits may involve the disclosure of CMI.

(7) Visits by foreign students enrolled in a DA or other DOD component educational institution or foreign national students participating in affiliation programs with Army facilities. However, these visits must be officially sponsored by the institution and arranged as an integral part of the students' curriculum. Such visits will only involve unclassified information.

(8) Visits by Canadian and Mexican government officials to DA organizations, agencies, activities, installations, and facilities in proximity to the borders of the U.S. However, these visits must be as a direct consequence of a mutual interest in preventing or resolving border-related incidents involving U.S. Army personnel. The goal is to maintain good community relations. Such visits will involve the disclosure of unclassified information only.

(9) Attendance at pre-bid briefings and bid opening ceremonies. Such visits will involve the disclosure of unclassified information. However, for closed briefings or ceremonies, the DA commander or agency head must have extended an invitation to foreign defense suppliers and foreign government representatives.

(10) Visits by foreign media representatives under the auspices of the Office of the Chief of Public Affairs, HQDA, or by the Office of the Assistant Secretary of Defense (Public Affairs). Such visits will involve the disclosure of public domain information only.

(11) Visits by foreign representatives of NATO and ABCA, accredited military attachés, participants in the U.S. Army-sponsored foreign dignitary program, and Limited Facility Clearance companies. Such visits may involve the disclosure of CMI. Visits by foreign nationals of Foreign-Owned U.S. companies and visits under the JCP will involve unclassified information only.

(12) Visits by commercial sales/marketing representatives for demonstrations/ presentations which will involve public domain information only.

(13) RDT&E activities will record all visits by foreign nationals engaged in technical information (see glossary) programs. This recording requirement applies exclusively to foreign nationals identified in paragraphs J-13a(4) and J-13a(9). At a minimum, the data elements cited below will be recorded and entered into a local database.

(a) Type of visit (one-time, recurring, or extended).

(b) Date of visit.

(c) Location/activity visited.

(d) Visitor.

1. Full name.

2. Date of birth.

3. Country of citizenship.
4. Sponsoring agency/organization.
5. Purpose of visit, such as contract number, project definition.
6. Level of U.S. information involved.

(e) MACOMs and agency heads will submit the above data through the ODCSINT, HQDA, website. Additionally, MACOMs and agency heads will—

1. Inform the supporting INSCOM element of visits in excess of 30 calendar days by the above-mentioned foreign nationals.

2. Prior to approval, provide medical research proposals, such as fellowships, to the Armed Forces Medical Intelligence Center.

b. The specific visits listed below are examples of the most common types of visits that a commander may encounter and approve under this delegated visit authority.

(1) *Visits by foreign subcontractors or foreign national employees of U.S. defense contractors.* Visits by foreign subcontractors or foreign national employees of U.S. contractors to DA elements or to DA contractor facilities on official business do not require a visit request through foreign government channels. Access to export controlled technical data in either case is authorized pursuant to an export license or by other written USG authorization obtained by the U.S. contractor. When the foreign subcontractor or foreign national employee visits a DA contractor facility or a DA element, the U.S. contractor will provide a copy of the written visit request accompanied by a copy of the export license or other documentation to the individual or agency to be visited with a copy furnished to the facility security office.

(2) *Visits for foreign participation in U.S. procurement-related meetings.* Potential foreign attendance must be assumed when planning for meetings that may lead to contract opportunities for nations with which the U.S. has reciprocal procurement agreements. Such meetings will involve only unclassified information.

(3) *Visits by representatives of the NATO.* One-time or recurring visits by representatives of NATO commands or agencies, or NATO International Staff, that involve access to NATO classified information, will be processed under U.S. Security Authority for NATO Affairs 1-69 (see DODD 5100.55) and do not require an embassy visit request. Visitors must be serving as representatives of their NATO organization for the purpose of engaging in specific NATO, not national, business. Clearance certification should be provided directly from the parent NATO organization to the meeting host, who will accomplish the necessary local coordination. Recurring visits related to NATO Production and Logistics Organizations or NATO Industrial Advisory Group Production Group (NIAG) activities will be processed according to AR 380-15. Note: Visits by representatives of a NATO command or agency or the NATO international staff, as well as personnel of NATO member countries, desiring to visit Army installations or Army contractor facilities to conduct business of a national nature or to attend conferences or meetings as a national representative must submit a visit request through embassy channels.

(4) *Visits by representatives of the American, British, Canadian, and Australian (ABCA) Armies Standardization Program.* Periodically, Army installations are required to provide a setting for ABCA meetings and to provide ingress and egress to the location. No disclosure issues are involved in that all U.S. information discussed in such a forum must have previously undergone proper disclosure review and be appropriately marked and authorized for disclosure to ABCA representatives. Representatives of ABCA wishing to visit Army installations to attend ABCA conferences or meetings, or to conduct ABCA specific business at that site, do not require an embassy-initiated visit request. Visitors must be serving as representatives to the ABCA Program for the purpose of engaging in specific ABCA, not national, business. Ingress and egress authority is to be coordinated directly between the office hosting the meeting or visit and the local foreign disclosure office, according to appendix H. Clearance certification will be provided directly from the parent ABCA member country to the U.S. Army meeting host, who will then effect all necessary coordination. Note: Foreign partner members of ABCA wishing to visit U.S. Army installations to conduct business of a national nature must submit a RVA through their respective embassies.

(5) *Canadian visits under the U.S.-Canada Joint Certification Program (JCP).* Under the U.S.-Canada JCP, procedures have been established to facilitate certain types of directly-arranged unclassified visits by Canadian government representatives and Canadian contractors to DA elements and DA contractor facilities. Further information on the JCP can be found in the DOD Pamphlet, "U.S.-Canada Joint Certification Program," published by the Office of the Under Secretary of Defense for Policy (OUSDP), dated March 1991, which is subject to ITAR limitations. All other visits by Canadian contractors not outlined in this subparagraph will be processed according to the self-invited visit procedures of this regulation. Canadian government officials and contractors are authorized to make direct visit arrangements with DA elements for the purpose of—

- (a) Responding to an invitation.
- (b) Collecting or discussing unclassified solicitations.
- (c) Furthering procurement activity related to unclassified solicitations (such as, pre-solicitation conferences).
- (6) *Military Attachés.*

- (a) The Director of Foreign Liaison, ODUSA(IA), HQDA officially recognizes certain foreign military officers as Military Attachés. A Military Attaché is acknowledged through accreditation to the U.S. Army as a diplomatic agent of

his or her government who is authorized to conduct official business concerning military matters with the U.S. Army. It should be noted that this recognition does not authorize a Military Attaché to interact officially with DA elements or personnel other than the Director of Foreign Liaison, ODUSA(IA); ODCSINT, HQDA; and Army Public Affairs, and the offices specified in the Letter of Special Accreditation (see glossary) furnished upon formal accreditation. Copies of the Letters of Special Accreditation given to the Military Attachés are provided to DA commands or agencies authorized to receive direct contact.

(b) Direct contact by telephone, letter, or visit to U.S. Army organizations or personnel other than the offices cited above, is not authorized unless the military attaché has received approval through a formal RVA.

(7) *Functions in honor of or sponsored by foreign representatives.* Periodically, U.S. Army installation commanders may be requested to provide a setting for functions in honor of or sponsored by foreign representatives. For functions in the Washington, DC area, these invitations will be received and distributed by ODUSA(IA), HQDA. Personnel receiving these invitations directly from a foreign representative will inform the ODUSA(IA), HQDA of the receipt of the invitation, and, in all cases, of their attendance plans to ensure the Army is properly represented at these functions.

(8) *Foreign-owned U.S. Companies.*

(a) Foreign-Owned U.S. Companies. Foreign-owned U.S. companies are not foreign companies. They are incorporated in the U.S. and are subject to U.S. laws and regulations, including the AECA and Export Administration Act (EAA). A U.S. wholly-owned subsidiary can represent its parent foreign company when doing business with either a U.S. Army organization or contractors doing business with the U.S. Army under the following conditions:

1. Visit requests, whether unclassified or classified, will be passed from the U.S. firm's security manager to the security manager of the U.S. Army organization or defense contractor.

2. If classified information is involved, there must be a contractual arrangement between the U.S. subsidiary and the parent (foreign) firm before such representation can take place.

3. There must also be a license in place or USG approval prior to the U.S. subsidiary sharing export controlled information or CMI with the parent company.

(b) Disclosure of CUI. There are no restrictions on disclosure to such foreign-owned companies of unclassified technical data controlled by the AECA or EAA, provided access within the company is limited to U.S. permanent residents. Any U.S. company, foreign-owned or U.S.-owned, must obtain the appropriate license or other written USG approval before the technical data can be exported or provided to a foreign national employee or other foreign person.

(c) Disclosure of CMI. Decisions on the disclosure of classified technical data to foreign-owned U.S. companies depend on the type of information involved and type of facility security clearance under which the company is operating. The most frequently employed arrangements to mitigate or negate foreign control or influence are as follows—

1. A voting trust is used to transfer legal control of a company to trustees, who are U.S. citizens. While the foreign owner retains equity ownership rights, the company is insulated from the foreign control and influence. Foreign nationals cannot have access to CMI or supervise classified contracts. There are no restrictions on access to CMI, provided the firm is cleared at the appropriate level and requires access to perform on a government contract.

2. A proxy arrangement provides for the legal title to remain with the foreign interests, but the company is nevertheless insulated from foreign control and influence. This arrangement, and access to CMI, is the same as the voting trust arrangement.

3. A special security agreement (SSA) allows the foreign parent firm to exercise general management. However, the day-to-day management of the company must be accomplished by U.S. citizens. Foreign nationals cannot have access to CMI or supervise classified contracts. When a contractor has been cleared under the SSA, the clearance is valid for use by all DOD components that may have a need to contract for classified work, subject to the provisions and limitations of each applicable agreement.

4. A company may be eligible for a limited facility clearance when the foreign ownership, control or influence (FOCI) stems from a country with which the U.S. has concluded a government-to-government security agreement that provides for this type of arrangement. Because foreign ownership or control remains in place and the company may employ foreign nationals, limited facility clearance companies may only have access to CMI determined to be releasable to the government of the ultimate parent company. Of the four types listed above, it is only in the case of a limited facility clearance firm that a foreign disclosure decision is required.

(9) Limited facility clearance company. A limited facility clearance company may prepare and submit RVAs directly to DA organizations, agencies, installations, facilities, contractors, or nongovernmental associations under DA security cognizance. These visits are processed under visit procedures outlined in DOD 5220.22-M. Access limitations imposed on a limited facility clearance contractor apply equally to all employees of such contractors. It is the responsibility of the visited agency to ensure that the access limitations of the limited facility clearance company are observed. Involvement of a foreign military attaché is not required.

(10) U.S.-Sponsored foreign dignitary visits. Foreign dignitaries are invited as guests of the Secretary of the Army, CSA, major commanders, HQDA principals in the name of the Secretary of the Army, CSA, Secretary of Defense, or CJCS. They may also be invited as part of security assistance or special programs. These visits may involve the expenditure of appropriated funds.

(a) DUSA(IA), HQDA role in U.S.-sponsored foreign dignitary and OT visits. DUSA(IA), HQDA is assigned overall staff responsibility for all U.S.-sponsored foreign dignitary visits and orientation tours (Ots). The DUSA(IA), in coordination with other interested staff agencies, will—

1. Plan and administer this DA program.
2. Ensure that all CMI disclosure issues are according to this regulation.
3. Administer visits (including planning when designated executive agent by DOD).
4. Serve as POC, providing advice and guidance in the selection of U.S. Army installations to be visited, when another military department is designated executive agent by DOD.
5. Coordinate directly with TRADOC and FORSCOM units for all tours or visits. TRADOC and FORSCOM will be information addressees on all messages tasking their activities.

(b) DUSA(IA), HQDA role in Latin America Cooperation Fund visits. ODUSA(IA), HQDA is responsible for overseeing LATAM Cooperation Fund visits, which are conducted at the unclassified level. ODUSA(IA), HQDA, will approve or deny (as necessary) the proposed visit concept submitted by the U.S. Army Military Attaché (ARMA) or SAO stationed in the appropriate Latin American country. Upon approval of the visit concept, the U.S. Army Attaché or SAO will effect direct coordination and submit formal notification to the CONUS-based U.S. Army activities to be visited.

(b) MACOMs and heads of HQDA staff agencies.

1. Must refer all inquiries regarding HQDA-sponsored visits and tours by foreign representatives (that is, CSA Counterpart Program) to ODUSA(IA), HQDA. When a proposed visit or tour is part of a separate program, coordination with DUSA(IA) will occur when original staff action is initiated.

2. Must be responsible for planning itineraries for visits or tours that fall within their responsibility, coordinating laterally, and conducting the tours.

J-14. Contact officer responsibilities

Contact officers will be designated in writing to facilitate and oversee activities of all foreign visitors at DA elements. Contact officers for one-time and recurring foreign visits will be designated in writing and will be physically accessible to the foreign personnel during the entire visit. The identification of the contact officer in the approved one-time, recurring, and extended RVAs satisfies the requirement for the contact officer to be named in writing, except for those EVAs under the programs cited in appendices K through O. Contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his duties. Contact officers also will adhere to the guidelines listed below. As a minimum, each contact officer is to perform the duties and functions outlined in this paragraph, which may be supplemented, as necessary, to meet local requirements. Note: In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the U.S. Army.

J-15. Visiting foreign representatives

Contact officers for visiting foreign representatives will—

a. Become familiar with chapters 1 through 4 of this AR, local supplementation, if any, and reportable foreign visitor activity under provisions of AR 381-12.

b. Be briefed by the FDO and become familiar with the specific scope and classification of the approved visit.

c. Coordinate with and obtain guidance from the following agency or command personnel:

(1) FDO (concerning the preparation of classified briefings or discussion items, in oral, visual, or documentary form (if requested by the visitors)).

(2) Security manager or OPSEC officer (concerning agency or command activities occurring simultaneously with the foreign visit and from which visitors should be excluded). Escorts are required when the visitors cannot otherwise be denied access to information or operations outside the scope of the approved visit.

(3) Protocol officer (concerning local policies regarding mandatory courtesy calls or exchange of mementos).

d. Prepare to receive and respond to confirmation of the visit and a possible request for administrative assistance by visitors or their military attachés.

e. On request, assist in arranging for quarters or transportation; however, it must be made clear to visitors or their military attachés that all expenses concerning the visit, including quarters, transportation, and subsistence, are the responsibility of the visitors. Because visits are occasionally canceled with little or no notice, contact officers should refrain from making commercial reservations for services on behalf of foreign visitors; rather, assistance should be limited to recommending and providing telephone numbers for commercial services to foreign visitors or their military attachés.

f. At the direction of the installation or activity commander, ensure that foreign visitors are aware of and comply with foreign disclosure and security requirements regarding the visit.

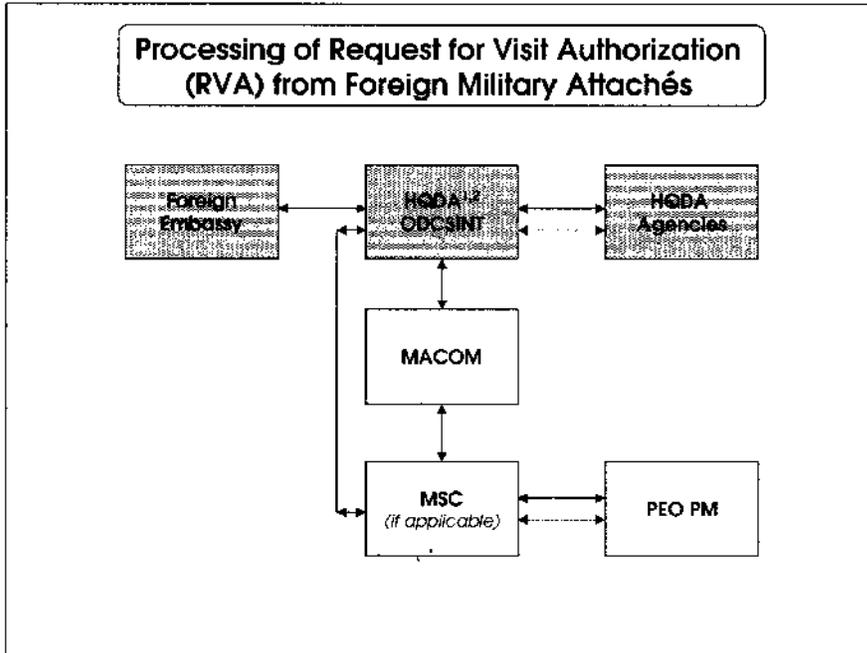
g. Personnel with whom the visitors have official contact or exchange information are made fully aware of information disclosure guidance and restrictions applicable to the visit.

h. Notify the supporting counterintelligence office of any foreign visitor activity that is reportable under the provisions of AR 381-12.

i. In the event of any misconduct on the part of a foreign visitor during the visit, provide a written report to ODCSINT, HQDA, through command channels.

J-16. Visits by FLOs, Foreign Exchange and CPP.

See appendices K through O.



- NOTES**
1. ODCSINT shall coordinate with HQDA proponent and affected agencies on RVAs to field units or activities. For example, a copy of a RVA to TRADOC on security assistance training will be sent to ODUSA(IA). These RVAs are initiated through FORDTIS, provided the Foreign Military Attaché is on-line.
 2. ODCSINT shall process all RVAs to PEO PMs through MSC Matrix Support and provide information copies to the directly affected MACOM.
- ↔ Action Tasker
 ↔ Coordination (as required)

Figure J-1. Processing of request for visit authorization (RVA) from foreign military attaches

Appendix K Foreign Liaison Officers

K-1. Concept

The Army FLO Program was established to facilitate cooperation and mutual understanding between the U.S. Army and armies of allied and friendly nations. A FLO is a foreign government military member or civilian employee, who is authorized by his or her government, and is certified by a DA command or agency in connection with programs, projects, or agreements of interest to the governments. FLOs are expected to present the views of their parent governments regarding issues of mutual interests, namely those that may be raised by the DA command or agency to which they are certified. Reciprocity is not required for the establishment of a FLO position. ODCSINT, HQDA is the DA proponent for this program.

a. Security Assistance. A foreign government representative, who is assigned to a DA command or agency pursuant to a requirement described in a FMS case. Note: This category of FLOs also includes foreign representatives that are assigned to a U.S. Army command or activity under ITOs to perform specific oversight functions of their respective foreign government's students. Certification forms and DDLs are mandatory for these foreign representatives.

b. Operational. A foreign government representative, who is assigned to a DA command or agency, pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education. For the purposes of this regulation, a StanRep is an operational FLO.

c. National Representative. A foreign government representative, who is assigned to his or her national embassy or legation in Washington, DC (for example, an accredited attaché or diplomatic member of an embassy, who is not formally accredited to the U.S. Army) to conduct liaison activities with DOD and DA.

K-2. Conditions and limitations

a. Certification by DA of FLOs does not bestow diplomatic or other special privileges, although certified FLOs may have diplomatic privileges based on an accreditation by the Department of State. FLOs will not act in the dual capacity as a representative of their government and as a foreign exchange personnel participant (for example, a MPEP, ESEP, or CPP) while assigned to a DA command or agency.

b. The activities of FLOs will be limited to representational responsibilities on behalf of their governments, as described in their certifications. FLOs will not perform activities that are the responsibility of employees of the DA organization to which they are assigned or represent the DA organization in any capacity. FLOs will not participate in non-representational activities or activities, such as airborne operations, piloting U.S. Army aircraft, or rappelling, unless specifically cited in an agreement or officially requested by the parent government and approved by ODCSINT, HQDA. Questions concerning the authorized activities of FLOs will be referred, through command or agency channels, to ODCSINT, HQDA, for resolution.

c. FLOs will not represent their governments as ATPOs in support of DEAs.

d. When the assignment of Security Assistance FLOs is accomplished pursuant to an LOA, USASAC will ensure that certain conditions and limitations are entered into the LOA. These conditions and limitations are at Figure K-1.

e. FLOs may assume temporary custody of authorized CMI documentary information to act as couriers (physical conveyance) only when they are authorized in writing by their government to assume responsibility as an agent of their government and ODCSINT, HQDA approval is granted.

(1) FLOs are not permitted to reproduce any U.S. CMI.

(2) They may have access to U.S. CMI authorized for disclosure to their government as defined in the individual certification form. Issuance of USG security containers for temporary storage of CMI may be authorized, but the supplied container and its contents will remain the responsibility of the U.S. installation's security office, to include the security combination.

f. FLOs' access to restricted areas will be according to AR 190-13 and local security policies and procedures and as specified in DDLs.

g. FLOs will not perform escort duties involving foreign visitors.

h. FLOs will wear their uniforms, if they are military personnel, or, if civilian, wear appropriate civilian attire. They also must wear, in clear view, a DOD building or installation pass or badge, if required, that clearly identifies them as foreign nationals and that is valid for a specific facility during normal duty hours. Any other identification (including organizational code and title, block, office nameplate, or e-mail address) used by or issued to FLOs by the host Army command or agency will clearly identify the FLO as a foreign representative. For example, an e-mail address will resemble the following: "SmithJ(Full country name Representative)@hqda.army. mil". Acronyms for country names

will not be used. The recipient of the FLO's e-mail message must be able to identify the FLO as a foreign representative.

i. While assigned to a DA/DOD installation, the FLOs will comply with all DOD, Service, command, and local installation rules and regulations.

j. All costs associated with the placement of a FLO at a DA installation are the responsibility of the FLO's parent government or international organization, including travel, office space, clerical support, quarters, rations, medical and dental services, and other administrative support costs, unless specifically stated otherwise in an applicable international agreement.

k. FLOs will be required to reside in CONUS at or within normal commuting distance of the organizational command or agency to which the FLO is certified.

K-3. FLO Memoranda of Agreement and Certification

a. *Memoranda of Agreement.* According to DODD 5230.20, when FLOs are physically assigned to U.S. Army installations in a security assistance or operational capacity, an agreement containing provisions concerning such matters as responsibilities and obligations of the parties, authorized activities, security requirements, financial arrangements and claims, must be executed. For the U.S. Army, this requirement is satisfied by an umbrella-type international agreement or an appropriate LOA negotiated and concluded on behalf of DA by ODCSINT, HQDA.

b. Certification.

(1) *Purpose.* FLOs are certified to a DA command or agency to perform specific functions on behalf of their governments under the auspices of an EVA. The purpose of such certification is to facilitate the timely accomplishments of a significant volume of routine business. Terms of certification are derived from and are consistent with the scope of existing international agreements or LOAs. FLOs are certified to an individual DA command or agency, specifically to further the objectives of such arrangements. The physical location of a FLO will be the DA command or agency that has implementation responsibility for the international agreement or FMS case to which the FLO is assigned. The exception to this rule is security assistance agreements involving a PEO weapon system. A MACOM may elect to execute a MOA with ASA(ALT) which would authorize the MACOM to transfer the FLO and associated security responsibility to ASA(ALT). Multiple certification as FLO to more than one command or agency is not authorized.

(2) *Certification at a Contractor Facility.* DA certification may be used to assign FLOs to a DOD activity at a contractor facility. If DA does not exercise this certification option, DA contractors desiring on-site representation must obtain authorization for the assignment of FLOs to their respective facilities through the export licensing process. The provisions of DOD 5220.22-M, chapter 10, apply. DA may choose to certify a FLO to a DOD activity at a contractor facility only if the following conditions are satisfied:

(a) The hosting facility agrees to the assignment in advance of any commitment.

(b) The Defense Security Service (DSS) and DA have agreed that the placement of the FLO at the facility will not jeopardize DA and or DOD CMI at the facility.

(c) DSS and DA have determined that appropriate controls can be put into place to ensure that the FLO's access is limited only to that which is authorized.

(d) DSS and DA agree on any security controls necessary to monitor and control access and on responsibility for the cost of such controls.

(e) The agreed controls are incorporated into a DDL, or equivalent written disclosure guidance, containing the data elements listed in appendix E of this regulation, and provided to DSS for continuing oversight purposes.

(3) *Certification Statement Form.* Each FLO must sign a certification statement acknowledging the terms of his or her assignment (see fig K-2). The contact officer is responsible for ensuring that the FLO understands and signs the certification statement form. A copy of the signed certification statement, which will be maintained at the local command or agency, must be provided to the FLO. If the FLO refuses to sign the certification statement, the contact officer will sign his or her portion of the form, annotate on the form that the FLO refused to sign the statement, provide a copy of the certification statement, signed by the contact officer, to the FLO, and notify ODCSINT, HQDA.

K-4. Establishment of FLO Positions and Processing of FLO Nominations.

a. *Establishment of FLO Positions.* DA commands and agencies desiring to have FLOs certified and assigned to them must formally obtain HQDA concurrence. A request for a new FLO position will not be approved unless the respective foreign government has signed a MOA or LOA. The procedures for establishing a new FLO position (see fig K-3) are as follows:

(1) *Request Initiated by a Foreign Government for Establishment of a FLO Position.*

(a) *Step 1:* If a foreign government initiates a request for the establishment of a FLO position with the U.S. Army, ODCSINT, HQDA will notify the affected command or agency in writing and request a recommendation on the establishment of the proposed FLO position. Such proposals will be conveyed in writing through command or agency channels. For example, if the request involves the assignment of a FLO to a PEO PM office, ODCSINT, HQDA will send the proposal to OASA(ALT) for staffing to the appropriate PEO PM.

(b) *Step 2:* The specified DA command or agency will evaluate the proposal and submit to ODCSINT, HQDA a recommendation to approve or disapprove the proposal. If the proposal involves the assignment of a FLO to the office of a PEO PM, the PM will coordinate his or her position with the MSC matrix support and submit the coordinated position to OASA(ALT) which will forward the response to ODCSINT, HQDA. FLO position proposals must provide a description with the following information:

1. Title of the position.
2. Position location.
3. Description of specific duties of the position.
4. Classified access level required.

5. Draft DDL or equivalent document containing data elements of a DDL. Note: According to DODD 5230.20, an equivalent document containing the information of a DDL is required for positions necessitating access to only unclassified information. The local commander may approve this disclosure document, with a copy furnished to ODCSINT, HQDA.

6. Clearly demonstrate a mutual need, actual or anticipated, for the position. The rationale must clearly demonstrate the requirement for the FLO's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve the best interests of the U.S. Army.

(c) *Step 3:* ODCSINT, HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: ODUSA(IA), OASA (ALT), Office of the DCSOPS (ODCSOPS), OTJAG, and the subject matter expert, if different from the preceding offices.

(d) *Step 4:* After HQDA coordination is completed, ODCSINT, HQDA will finalize the decision on the proposal and formally notify the appropriate foreign government embassy. If the proposal is approved, the DA command or agency to which the FLO will be assigned will immediately begin to finalize the position DDL for approval and issuance by ODCSINT, HQDA. Upon receipt of the final draft DDL proposal, ODCSINT, HQDA will staff the final draft DDL with the HQDA offices cited in Step 3 (above) and other appropriate agencies. Upon concurrence and approval of the DDL, ODCSINT, HQDA, will notify the hosting Army command or agency and the appropriate foreign military attaché. The approved DDL will be in place prior to the submission of the EVA request by the appropriate foreign military attaché.

(2) *Request Initiated by a DA Command or Agency for Establishment of a FLO Position.*

(a) *Step 1:* Prior to beginning discussions with foreign representatives on the establishment of a FLO position, DA commands or agencies must obtain ODCSINT, HQDA permission to proceed. Such proposals will be conveyed in writing through command or agency channels to ODCSINT, HQDA. Proposals conveyed through PEO PMs will be sent to OASA(ALT) for forwarding to ODCSINT, HQDA.

(b) *Step 2:* A DA command or agency will provide the following information to support its initiative to establish a FLO position:

1. Title of the position.
2. Position location.
3. Description of specific duties of the position.
4. Classified access level required.

5. Draft DDL or equivalent document containing data elements of a DDL. Note: According to DODD 5230.20, an equivalent document containing the information of a DDL is required for positions necessitating access to only unclassified information. The local commander may approve this disclosure document, with a copy furnished to ODCSINT, HQDA.

6. Clear statement of need for the position. The rationale must clearly demonstrate the requirement for the FLO's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve the best interests of the U.S. Army.

(c) *Step 3:* ODCSINT, HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: ODUSA(IA), OASA (ALT), Office of the DCSOPS (ODCSOPS), OTJAG, and the subject matter expert, if different from the preceding offices.

(d) *Step 4:* After HQDA coordination is completed, ODCSINT, HQDA will finalize the decision on the initiative and formally submit the proposal to the appropriate foreign government embassy. If the latter is receptive to the proposal, ODCSINT, HQDA will direct the negotiations for DA. While the negotiations are being conducted, the DA command or agency that initiated the proposal will immediately begin to finalize the draft position DDL for approval and issuance by ODCSINT, HQDA. Upon receipt of the final draft DDL, ODCSINT, HQDA will staff the document with the HQDA offices cited in Step 3 (above) and other appropriate agencies. Upon concurrence and approval of the DDL by ODCSINT, HQDA, the latter will hold the document awaiting conclusion of the negotiations and formal agreement to establish a FLO position. Upon establishment of the FLO position, the approved DDL will already be in place awaiting the submission of the EVA request by the appropriate foreign military attaché.

b. Processing of FLO Nominations. If the FLO position is established, ODCSINT, HQDA will process the assignment of the FLO to a DA command or agency (see fig K-4) in the following manner:

(1) *Step 1:* The appropriate foreign military attaché will submit an EVA request at least 45 days prior to the requested date of arrival/assignment of the FLO. In the EVA request, the foreign military attaché provides written notification to ODCSINT, HQDA of the following—

(a) The individual is an officially-sponsored representative of that government.

(b) The official is authorized by the sponsoring government to conduct business with DA for purposes that must be specific, citing related agreements, contracts, or other arrangements that establishes acceptance of the FLO position.

(c) The official's legal status (including any privileges and immunities to which the individual is entitled).

(d) The official holds a specified level of security clearance.

(e) The official may assume temporary custody of CMI documentary information for courier purposes.

(f) The parent government will assume the responsibility for any and all U.S. CMI provided to the FLO.

(2) *Step 2:* ODCSINT, HQDA will process the EVA request to the DA command or agency (PEO PM through its matrix support) to which the FLO is to be assigned. Since the position DDL outlining the terms of the certification of the FLO was pre-coordinated and approved, the recipient DA command or agency should respond favorably within 20 working days of the receipt of the EVA request. The position DDL will remain valid until there is a change to the scope of the position or the position is terminated. See appendix E for detailed information on DDLs.

(3) *Step 3:* Upon receipt of the concurrence of the recipient DA command or agency (PEO PM through its matrix support), ODCSINT, HQDA will approve the EVA request and notify the recipient DA command or agency of the approval. The foreign military attaché will then coordinate with the recipient DA command or agency for the arrival of the FLO. Note: DA commands or agencies may not accept a FLO until the DDL and visit request have been approved. If a FLO arrives prior to visit approval, the DA command or agency involved will not permit the FLO to commence his or her duties. The DA command or agency FDO must be notified immediately. The DA command or agency FDO will then notify the ODCSINT, HQDA, who will coordinate the disposition of FLO with the appropriate foreign military attaché and provide instructions to the DA command or agency FDO.

c. Modification of a FLO Position. Any proposal to change the scope of a FLO's certification will be according to the procedures outlined in paragraphs K-4a(1) and K-4a(2), with emphasis on the specific modification. Any proposal to extend the FLO's duration must be initiated and requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

d. Reevaluation of a FLO Position. Once established, each FLO position and the associated position DDL will be reevaluated on each successive nomination to ensure that the best interests of the host command or agency and DA continue to be served, and the purpose of the position remains valid. To alleviate the possibility of a FLO arriving to assume an established position prior to visit approval, ODCSINT, HQDA will initiate contact with the appropriate foreign government Military Attaché in Washington, DC, 90 days prior to the tour expiration date of the incumbent FLO and query the foreign military attaché concerning a replacement for the position, extension of the incumbent FLO, or other alternatives contemplated by the parent government. The ODCSINT, HQDA will also inform the sponsoring Army command or agency of the intended action, if any, of the foreign government to alter the status of the FLO position. The host command or agency FDO and contact officer will also commence their reevaluation 90 days prior to the tour expiration date of the incumbent FLO.

K-5. Administering FLOs

a. Visits.

(1) Visits by FLOs may be approved by the contact officer, provided the proposed destination is within the organizational jurisdiction of DA and the purpose of the visit is within the scope of the FLO's approved terms of certification. The contact officer is required to coordinate such visits between activities and these visits do not require official authorization from ODCSINT, HQDA.

(2) All visits by FLOs to destinations outside the terms of certification must be initiated on the FLO's behalf by their military attaché through the FVS.

(3) All visits by FLOs to destinations outside DA jurisdiction (that is, destinations under the organizational jurisdiction of other services, OSD, JCS - including unified and specified commands - and other Federal departments and agencies), but within the terms of certification will be coordinated by the FLO's contact officer. The contact officer will comply with the procedures of the proposed host organization for the visit. For example, the proposed host organization may require a letter of request from the FLO's parent embassy. In such cases, the contact officer should have the FLO notify his or her embassy of the proposed host organization's requirements and obtain the proper documentation for submission to the host organization.

(4) Travel-related funding for all FLO visits is the exclusive responsibility of the FLO's parent government. The provisions of AR 95-1 govern travel on U.S. military aircraft by FLOs.

b. Library and Publications Support. At the discretion of the host activity's contact officer, a FLO may be granted supervised access to unclassified (to include CUI) sections of a command or agency libraries. Additionally, each FLO

may be provided a reference set of DA and activity publications necessary to the successful performance of the FLO's duties, consistent with the FLO's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the FLO's successor when the FLO's certification ends.

c. Computer Access. FLOs may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is authorized for disclosure to their government. See paragraph K-2h for information regarding e-mail addresses and messages. In all cases, the provisions of AR 380-19 and local security procedures will apply.

d. Misconduct. FLOs serve at the pleasure of DA and must conform to the Army's customs and traditions and comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If a FLO violates the terms of certification, violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the contact officer will notify the local agency or command FDO and provide a written report regarding the inappropriate action, through command channels, to ODCSINT, HQDA, with a recommendation for final disposition by HQDA, such as temporary suspension or permanent revocation of privileges, or revocation of certification. ODCSINT, HQDA will coordinate the resolution of all cases involving FLO misconduct.

K-6. U.S. Contact Officer

a. Contact officers will be designated, in writing, by the commander, agency head, or designee to facilitate and oversee the activities of FLOs at DA commands or agencies. The contact officer should be of equivalent rank/grade or higher, if available, to the FLO. A primary and an alternate contact officer must be identified in the DDL. Contact officers must be physically accessible to and have daily contact with the FLO. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his or her duties. Contact officers will also comply with the guidelines listed below. Note: In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the U.S. Army.

b. The contact officer for a FLO will—

(1) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by ODCSINT, HQDA for the individual FLO position.

(2) Initially brief a new FLO on DA and local policies and procedures affecting the FLO's status and performance of functions, as well as customs of the U.S. Army; subsequently, the contact officer will render advice and assistance to the FLO in complying with such policies and procedures. The contact officer will have the FLO sign a statement, similar to the document exhibited at figure K-2, indicating his or her agreement and understanding. The contact officer will provide a copy of the signed certification form to the FLO.

(3) In conjunction with the FDO, evaluate the FLO's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the FLO's approved terms of certification. Consultations and visits beyond a FLO's terms of certification require the submission of formal visit requests by the FLO's embassy in Washington, DC.

(4) Receive, evaluate, and recommend/refer all FLO requests for CMI to the FDO.

(5) Receive, evaluate, and refer all FLO requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent, who will render a disclosure decision and return the action to the FDO for case closure.

(6) Notify the ODCSINT, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of FLOs under their oversight.

(7) Notify the supporting counterintelligence and local security offices of any foreign visitor activity which is reportable under the provisions of AR 381-12.

(8) Comply with the procedures cited in paragraph K-5d of this appendix regarding misconduct on the part of the FLO.

(9) Brief U.S. personnel with whom the FLO will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

K-7. National Representatives

A foreign national representative will submit a recurring visit request when he or she visits a DA command or agency on a frequent basis for a specific project. In these cases, the foreign national representative will be acting as a FLO. However, a DDL will not be issued. Instead, all disclosure guidance and delegated disclosure authorization to the hosting command or agency will be entered on the RVA and issued upon the approval of the recurring visit request.

K-8. Administrative Support Personnel

a. Administrative support personnel for FLOs will not be permitted to act on behalf of the supported FLO (that is, sign for documents, attend meetings without the supported FLO, etc.) or represent the foreign government. The use of

these administrative support personnel is to be approved solely for the limited purpose of assisting the FLO in clerical and secretarial matters.

b. There are two authorized categories of individuals, who may be hired to serve as administrative support personnel:

(1) *Foreign Nationals*. If the individual is a foreign national hired directly by the foreign government, the administrative support person must be nominated by the foreign embassy on an extended visit request. However, a visit request is not required for an administrative support person if access to a U.S. Army activity or installation is not necessary (that is, FLO office is not located on a U.S. Army activity or installation). There are two types of foreign nationals that may be hired by FLOs as administrative support personnel: (1) individuals in the U.S. on a work visa or (2) individuals (that is, spouses of military attachés or FLOs) that have been granted waivers to work by both the Department of State and the Immigration and Naturalization Service.

(2) *U.S. Persons*. If a private U.S. citizen or a permanent resident has been hired by the foreign government on a full-time basis to perform administrative support to a FLO, no visit request is required. However, the host command or agency will provide written notification to ODCSINT, HQDA of the hiring if access (ingress and egress) to the installation is required.

c. A private U.S. person working as an administrative support person for a FLO must be granted a foreign government security clearance to support the position, if access to CMI is required. The security clearance will be certified to the U.S. Army through a RVA. However, access to CMI will be limited to that classified information which has been properly cleared and disclosed to the FLO. Therefore, the administrative support person will not have access to U.S. CMI other than through the supported FLO.

d. Administrative support person (except those persons cited in paragraph K-8h) that require ingress and egress to restricted areas on an installation will be issued a foreign representative badge.

e. E-mail addresses with “.mil” extension will not be issued to administrative support persons.

f. The parent government embassy in Washington, DC will submit an RVA for travel of any administrative support person (regardless of nationality) to other U.S. Army facilities in the company of the FLO.

g. DDLs are not required for administrative support persons.

h. Note: In the event that a U.S. civil servant is assigned to duties as an administrative support person to a FLO, he or she may retain the U.S. security badge as well as the .mil e-mail access. It will be incumbent on that individual to ensure the supported FLO does not have access to the “.mil” e-mail system and the information accessed through the “.mil” address is not disclosed to the FLO. The commander or agency head will be responsible for notifying USASAC of the assignment of any U.S. civil servant to support a FLO. The purpose of this notification is to effect reimbursement procedures.

In the absence of an umbrella LNO MOA in effect between DA and the country concerned, USASAC will ensure that the following standardized conditions and limitations are entered into the LOA for FLOs.

1. The Liaison Officer will represent the Parent Party to the Host Party. The Liaison Officer will not perform duties reserved by the laws or regulations of the Host Government to officers or employees of the Host Government, nor will the Liaison Officer provide any labor or services to the Host Government or any of its agencies, including the Host Party.
2. The Liaison Officer will comply with all applicable Host Country policies, procedures, laws and regulations. The Host Party will assign a Contact Officer to provide guidance to the Liaison Officer concerning requirements of the Host Party and to arrange for activities consistent with such requirements and the purposes of this LOA.
3. The Liaison Officer may request access to Host Party facilities if such access promotes the purposes of this LOA, is consistent with the terms of any applicable formal certification or approval issued by the Host Country, and is permitted under the applicable laws and regulations of the Host Country. Such requests will be submitted to the Contact Officer. Approval of such requests will be at the discretion of the Host Country. Any request for access that exceeds the terms of an applicable certification or approval will be submitted through diplomatic channels.
4. The Liaison Officer will not be granted access to information of the Host Party, whether or not classified, except as authorized by the Host Party, and only to the extent necessary to fulfill the Liaison Officer's functions herein.
5. All information to which the Liaison Officer is granted access while serving as a liaison to the Host Party will be treated as information provided to the Parent Government, in confidence, and will not be further released or disclosed by the Liaison Officer to any other person, firm, organization, or government without the prior written authorization of the Host Government. Disclosure of information to the Liaison Officer will not be deemed to be a license or authorization to use such information for any purpose other than the purposes described herein.
6. The Liaison Officer will not be assigned to locations where hostilities are likely. Should hostilities occur at a location where the Liaison Officer is assigned, the Host Party will promptly remove the Liaison Officer to a location where involvement by the Liaison Officer in such hostilities is unlikely.

Figure K-1. FLO LOA conditions and limitations

-
7. The Liaison Officer will not participate in exercises or civil-military actions, unless expressly authorized to do so by both the Host and Parent Party.
 8. The Liaison Officer will comply with the dress regulations of the Parent Party, but, if requested by the Host Party, will also wear such identification as may be necessary to identify the Liaison Officer's nationality, rank and status as a Liaison Officer. The order of dress for any occasion will be that which most closely conforms to the order of dress for the particular unit of the Host Party, which the Liaison Officer is serving. The Liaison Officer will comply with the customs of the Host Party with respect to the wear of civilian clothing.
 9. Prior to the commencement of a Liaison Officer's tour, the Parent Party will notify the Host Party of the specific Parent Party organization which will exercise operational control over the Liaison Officer and, if different, the Parent Party organization that will provide administrative support to the Liaison Officer and the Liaison Officer's dependents.
 10. At the end of a Liaison Officer's tour, or as otherwise agreed by the Parties, the Parent Party may replace the Liaison Officer with another individual who meets the requirements of this LOA. Such replacement will be subject to any certification or approval requirements imposed under the laws and regulations of the Host Party.
 11. The Host Party's certification or approval of an individual as a Liaison Officer will not, in and of itself, bestow diplomatic or other special privileges on that individual.
 12. The Host Party will establish the maximum substantive scope and classification levels within which the disclosure of any classified information or controlled unclassified information to the Liaison Officer will be permitted. The Host Party will inform the Parent Party of the level of security clearance required to permit the Liaison Officer access to such information.
 13. Each Party will cause security assurances to be filed stating the security clearances for the Liaison Officer being assigned by such Party. The security assurances will be prepared and forwarded through prescribed channels in compliance with established Host Party procedures.
 14. The Parent Party will ensure that each assigned Liaison Officer is fully cognizant of, and complies with, applicable laws and regulations concerning the protection of proprietary information (such as patents, copyrights, know-how, and trade secrets), classified information and controlled unclassified information disclosed to the Liaison Officer. This obligation will apply both during and after termination of an assignment as a Liaison Officer. Prior to taking up duties as a Liaison Officer, the Liaison Officer will be required to sign the certification form. Only individuals who execute the certification form will be permitted to serve as Liaison Officers.

Figure K-1. FLO LOA conditions and limitations—Continued

15. The Parent Party will ensure that the Liaison Officer, at all times, complies with the security laws, regulations and procedures of the Host Government. Any violation of security procedures by a Liaison Officer during his or her assignment will be reported to the Parent Party for appropriate action. Upon request by the Host Party, the Parent Party will remove any Liaison Officer who violates security laws, regulations, or procedures during his or her assignment, or fails to display a commitment to comply with such laws, rules, or procedures.

16. All classified information made available to the Liaison Officer will be considered to be classified information furnished to the Parent Party, and will be subject to all provisions and safeguards provided for under the General Security of Military Information Agreement (GSOMIA) or equivalent security arrangement.

17. The Liaison Officer will not take custody of classified information in tangible form (for example, documents or electronic files), except to act as a courier and as expressly permitted by the terms of the formal certification or approval of the Liaison Officer and as authorized by the Parent Government.

18. The obligations of the Liaison Officer and the Parent Party with respect to classified or controlled unclassified information disclosed by the Host Party in connection with this Agreement will survive termination or expiration of this LOA.

19. Consistent with the laws and regulations of the Host Government and this Agreement, the Liaison Officer will be subject to the same restrictions, conditions, and privileges as Host Party personnel of comparable rank and in comparable assignments. Nothing herein will limit any exemption from taxes, customs or import duties, or similar charges available to the Liaison Officer or the Liaison Officer's dependents under applicable laws and regulations or any international agreement between the Host Government and the Parent Government.

20. Unless otherwise agreed by the Parties, the Liaison Officer will reside within commuting distance from the Host Party unit or office with which the Liaison Officer is serving as a liaison.

21. Neither the Host Party nor the armed forces of the Host Government may take disciplinary action against a Liaison Officer who commits an offense under the military laws or regulations of the Host Party, nor will the Host Party exercise disciplinary authority over the Liaison Officer's dependents. The Parent Party, however, will take such administrative or disciplinary action against the Liaison Officer, as may be appropriate under the circumstances, to ensure compliance with this Agreement, and the Parties will cooperate in the investigation of any offenses under the laws or regulations of either Party.

22. The certification or approval of a Liaison Officer may be withdrawn, modified or curtailed at any time by the Host Party for any reason, including, but not limited to, the violation of the regulations or laws of the Host Party or the Host Government. In addition, at the request of the

Figure K-1. FLO LOA conditions and limitations—Continued

Host Party, the Parent Government will remove the Liaison Officer or a dependent of the Liaison Officer from the territory of the Host Country. The Host Party will provide an explanation for its removal request, but a disagreement between the Parties concerning the sufficiency of the Host Party's reasons will not be grounds to delay the removal of the Liaison Officer or his/her dependent. If so requested by the Host Party, the Parent Party will replace any Liaison Officer removed under this paragraph, provided the replacement meets the requirements of this LOA.

23. A Liaison Officer will not exercise disciplinary or supervisory authority over military or civilian personnel of the Host Party.

Figure K-1. FLO LOA conditions and limitations—Continued

[Office Symbol]

[Date]

SECTION I
LIAISON OFFICER
LEGAL STATUS OF CERTIFICATION

As a representative of the [foreign organization] under the auspices of an Extended Visit Authorization to the United States Army, I am subject to the jurisdiction of United States Federal, State, and local laws, except as provided by treaty, other specific legal authority, or the terms of any diplomatic immunity which I may have been granted. I understand that my acceptance of the Liaison Officer position does not bestow diplomatic or other special privileges.

SECTION II
LIAISON OFFICER
CONDITIONS OF CERTIFICATION

- (1) Responsibilities: I understand that my activities will be limited to the representational responsibilities of my government and that I am expected to present the views of my government with regard to the issues which my government and the U.S. Government have a mutual interest. I will not perform duties that are reserved by law or regulation to an officer or employee of the U.S. Government.
- (2) Costs: I understand that all costs associated with my duties as a Liaison Officer will be the responsibility of my government, including, but not limited to, travel, office space, clerical services, quarters, rations, and medical and dental services.
- (3) Extensions and Revalidation: I understand that if my government desires to request an extension or revalidation of my position beyond the original dates for which I am certified, a new visit request will be submitted not later than 30 days prior to the expiration date of the current Extended Visit Authorization.
- (4) Contact Officer: I understand that when the certification process is completed, a Contact Officer(s) will be assigned to sponsor me during my visit to the United States Army. I further understand that I will coordinate, through my Contact Officer, all requests for information, visits, and other business, which fall under the terms of my certification. I also understand that requests for information, which are beyond the terms of my certification, will be made through the Office of the Defense Attaché.

Figure K-2. Sample certification

(5) Other Visits: I understand that visits to facilities for which the purpose does not directly relate to the terms of my certification will be made through the Office of the Defense Attaché.

(6) Uniform: I understand that I will wear my national uniform or appropriate civilian attire when conducting business at the [location of the United States Government facility] or other Department of Defense facilities, unless otherwise directed. I will comply with my Parent Government's service uniform regulations.

(7) Duty Hours: I understand that my duty hours are Monday through Friday, from (TIME) to (TIME). Should I require access to my work area during non-duty hours, I am required to request permission from the command security officer. I further understand that (IT IS) (IT IS NOT) necessary to assign a United States escort officer to me during my non-duty access. Any cost incurred as a result of such non-duty access may be reimbursable to the United States Government.

(8) Administrative Support Personnel: Should I elect to employ an administrative support person, I understand and agree to the following conditions:

a. I understand that I must brief my administrative support person on his or her duties and conditions of employment, to include his or her conduct within an activity of the United States Army.

b. I understand that my administrative support person will not be permitted to act on my behalf or represent my government.

c. I understand that any security clearance associated with my administrative support person will be sponsored and issued by my parent government.

d. I understand that my administrative support person, if a foreign national, will have the appropriate status to work in the United States. This work status is defined by the Department of State in conjunction with the United States Immigration and Naturalization Service.

(9) Security:

a. I understand that access to U.S. Government information will be limited to that information determined by my Contact Officer to be necessary to fulfill the functions of a Liaison Officer. I also understand that I may not have unsupervised access to U.S. Government computer systems, unless the information accessible by the computer is releasable to my government according to applicable U.S. law, regulations and policy.

Figure K-2. Sample certification—Continued

b. All information to which I may have access during my certification will be treated as information provided to my government in confidence and will not be further disclosed or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the United States Government.

c. I understand that all classified material (United States or Parent Government) is to remain under the control of the Host Party and is subject to inspection by Host Party security officials. This does not preclude issuance of a security container for temporary storage of Classified Information if justification exists and is consistent with the terms of my certification. The Host Party supplied container and its contents will remain the responsibility of the Host Party, to include the security combination.

d. While assigned to (U.S. Army organization), I will comply with all United States Army administrative rules and security regulations. I understand that my office is subject to safety and security inspections.

e. I may not reproduce U.S. classified information for which I have assumed temporary custody. I am authorized to reproduce controlled unclassified information.

f. I will immediately report to both my contact officer should I obtain or become knowledgeable of United States Government information for which I am not authorized to have access. I further agree that I will report to my contact officer any incidents of my being offered or provided information that I am not authorized to have.

g. If required, I will display a security badge on my outer clothing so that it is clearly visible. The United States Government will supply this badge.

(10) Compliance: I have been briefed on, fully understand, and will comply with the terms and conditions of my certification. Failure to comply may result in termination of my certification. I further understand that the termination of my certification does not preclude further disciplinary action according to any applicable Status of Forces Agreement or other government-to-government agreements.

(11) Terms not defined herein will have the definitions ascribed to them in the applicable Agreement governing my assignment as a Liaison Officer.

Figure K-2. Sample certification—Continued

SECTION III
LIAISON OFFICER
TERMS OF CERTIFICATION

- (1) Contact Officer: (NAME OF CONTACT OFFICER[s]) has been assigned as my contact officer.
- (2) Certification: I am certified to the [DOD Service, agency or organization] in support of the following programs/topics/etc.
- (3) Travel: I may visit the following locations under the terms of my certification, with the permission of my Contact Officer:

SECTION IV
LIAISON OFFICER
CERTIFICATION OF IN-BRIEFING

I, (NAME OF LIAISON OFFICER), understand and acknowledge that I have been certified as a Liaison Officer to the [DOD Service, agency or organization], as agreed upon between the [Foreign Organization] and the United States [DOD Service, agency or organization]. I further acknowledge that I fully understand and have been briefed on: (1) the legal status of my certification; (2) the conditions of my certification; and (3) the terms of my certification. I further acknowledge that I will comply with the conditions and responsibilities of my certification.

SIGNATURE OF LIAISON OFFICER

DATE

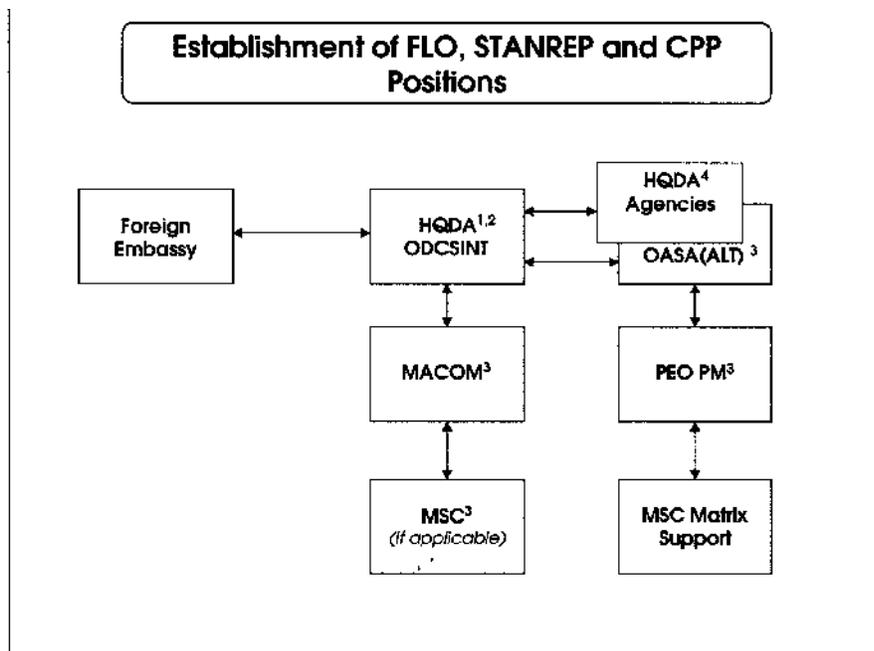
TYPED NAME OF LIAISON OFFICER

SIGNATURE OF BRIEFER

RANK AND OR TITLE

TYPED NAME

Figure K-2. Sample certification—Continued



- NOTES**
1. Effect HQDA coordination in all cases.
 2. Provide information copy of all requests involving proposed establishment of positions with PEO PMs.
 3. If the request for the establishment of a FLO position originates from a DA element, the action shall be processed through command channels to ODCSINT, HQDA or from a HQDA agency directly to ODCSINT, HQDA.
 4. ODUSA(IA), HQDA shall initiate and coordinate or receive (from ODCSINT) and coordinate all taskers involving the establishment of StanRep positions.
- ↔ Action Tasker
 ↔ Coordination (as required)

Figure K-3. Establishment of FLO, StanRep and CPP positions

Appendix L Standardization Representatives

L-1. Concept

a. The American, British, Canadian, Australian Armies' Standardization (ABCA) Program began in 1947 when General Eisenhower and Field Marshall Montgomery agreed that the levels of cooperation and standardization achieved during World War II should be maintained and extended. Since that original agreement the ABCA Program has produced over 1000 standardization agreements, known as Quadripartite Standardization Agreements (QSTAGs) and Quadripartite Advisory Publications (QAPs). The current ABCA Program is based upon the Basic Standardization Agreement of 1964, which provides for the unencumbered exchange of information, equipment, and personnel between and among participating countries.

b. The aim of the program is the achievement of levels of standardization by—

- (1) Ensuring the fullest cooperation and collaboration among Armies,
- (2) Achieving the highest possible degree of interoperability among Armies through materiel and non-materiel standardization, and
- (3) Obtaining the greatest possible economy by the use of combined resources and effort. To reflect the changing role of its Armies, the Program has now put in place a strategy to support these goals. This is "to ensure that Armies achieve agreed levels of standardization necessary for two or more ABCA Armies to operate effectively together within a coalition."

c. The purpose of the ABCA Program is—

- (1) To keep each army fully informed of research and development taking place in the other armies,
- (2) To guide research and development whenever possible along lines compatible with the requirements of all four Armies,
- (3) To record and maintain formal agreements in both the materiel and non-materiel fields on items or concepts acceptable to two or more Armies, and
- (4) To ensure such formal agreements are not modified without consultation.

d. A StanRep is an operational FLO certified by the U.S. Army to represent the British, Canadian, or Australian government under the authority of the Basic Standardization Agreement. Each of the participating Armies provides StanReps to other Armies as desired to conduct liaison between the "parent" Army and the "host" Army in pursuit of ABCA goals and objectives. Placement of British, Canadian, and Australian StanReps in the U.S. is governed by U.S. policy on FLOs, specifically DODD 5230.20 and this regulation. The DA proponent for this program is ODUSA(IA).

e. Senior National Officers and Washington Standardization Officers develop a Corporate Plan every 2 years, which provides priority areas of focused activity. The ABCA Program encompasses all Battlefield Operating Systems. Each of the participating Armies appoints a NSO, who serves as his nations "program manager". The U.S. NSO is assigned to ODUSA(IA).

f. Quadripartite Working Groups (QWGs) are formed to exchange information and work on improving the capability of ABCA Armies to operate together. QWGs develop Program Plans of Action which describe their standardization activities. Many of the QWG activities result in QSTAGs or QAPs. They also develop a "standardization list" (StanList), which identifies programs and specific documents that Armies have agreed to share with the other participating Armies. U.S. items placed on the StanList must undergo the normal foreign disclosure approval process as cited in this regulation before being placed on the StanList. QWGs can form subordinate Special Working Parties and Information Exchange Groups, with the approval of the Washington Standardization Office, to work on specific tasks. Participating Armies appoint National Points of Contact to each of the QWGs to serve as national subject matter experts to the working group; other delegates and representatives are selected as required.

L-2. Conditions and Limitations

a. Certification of a StanRep does not bestow diplomatic or other special privileges, although certified StanReps may have diplomatic privileges based on an accreditation by the Department of State. StanReps will not act in the dual capacity as a representative of their government and as a foreign exchange personnel participant (for example, a MPEP, ESEP, or CPP) while assigned to a DA command or agency.

b. The activities of StanReps will be limited to representational responsibilities for their government as prescribed in the certification; they may not perform activities that are the responsibility of employees of the organization to which assigned or represent the organization in any capacity.

c. StanReps will not represent their governments as ATPOs in support of DEAs.

d. StanReps may assume temporary custody of authorized CMI documentary information to act as couriers (physical

conveyance) only when they are authorized in writing by their government to assume responsibility as an agent of their government and ODCSINT, HQDA approval is granted.

(1) StanReps are not permitted to reproduce any U.S. CMI.

(2) They may have access to U.S. CMI authorized for disclosure to their government as defined in the individual certification form. Issuance of USG security containers for temporary storage of CMI may be authorized, but the supplied container and its contents will remain the responsibility of the U.S. installation's security office, to include the security combination.

e. StanReps' access to restricted areas will be according to AR 190-13 and local security policies and procedures and as specified in DDLs.

f. StanReps will not perform escort duties involving foreign visitors.

g. StanReps will wear their uniforms, if they are military personnel, or, if civilian, wear appropriate civilian attire. They also must wear, in clear view, a DOD building or installation pass or badge (if required) that clearly identifies them as foreign nationals and that is valid for a specific facility during normal duty hours. Any other identification (including organizational code and title, block, office nameplate, or e-mail address) used by or issued to StanReps by the host Army command or agency will clearly identify the person's status as a foreign representative. For example, an e-mail address will resemble the following: "SmithJ(full country name Representative)@hqda.army. mil". Acronyms for country names will not be used. The recipient of the StanRep's e-mail message must be able to identify the StanRep as a foreign representative.

h. While assigned to a DA/DOD installation, the StanReps will comply with all DOD, Service, command, and local installation rules and regulations.

i. All costs associated with the placement of a StanRep at a DA installation will be according to the Basic Standardization Agreement of 1964.

j. StanReps that are assigned to a specific U.S. Army command or agency will be required to reside in CONUS at or within normal commuting distance of the organizational command or agency to which certification is proposed.

L-3. StanRep Memoranda of Agreement and Certification

a. *Memoranda of Agreement.* The Basic Standardization Agreement of 1964 governs the assignment of StanReps to the Primary Standardization Office. StanReps assigned to DA commands or agencies are assigned, pursuant to MOA or LOA, as operational FLOs according to 5230.20 and this regulation. A request for a new StanRep position at a DA command or agency will not be approved unless the respective foreign government has entered into a LNO MOA or an appropriate LOA.

b. *Certification.*

(1) *Purpose.* StanReps are certified to a DA command or agency to perform specific functions on behalf of their governments under the auspices of an EVA. The purpose of such certification is to facilitate the timely accomplishments of a significant volume of routine business. Terms of certification are derived from and are consistent with the scope of the Basic Standardization Agreement of 1964. StanReps are certified to an individual DA command or agency, specifically to further the objectives of this standardization agreement. Multiple certification of a StanRep to more than one command or agency is not authorized.

(2) *Certification Statement.* Each StanRep must sign a certification statement acknowledging the terms of his or her assignment (see fig L-2). The contact officer is responsible for ensuring that the StanRep understands and signs the certification statement. A copy of the signed certification statement, which will be maintained at the local command or agency, must be provided to the StanRep. If the StanRep refuses to sign the certification statement, the contact officer will sign his or her portion of the statement, annotate on the form that the StanRep refused to sign the statement, and provide a copy of the certification statement, signed by the contact officer, to the StanRep, and notify ODCSINT, HQDA.

L-4. Establishment of StanRep Positions and Processing of StanRep Nominations

a. *Establishment of StanRep Positions.* DA commands and agencies desiring to have StanReps certified and assigned to them must formally obtain HQDA concurrence. A request for a new StanRep position will not be finalized unless both parties agree to the establishment of the new StanRep position. The procedures for establishing a new StanRep position (see fig K-3) are as follows:

(1) Request initiated by a foreign government for establishment of a StanRep position.

(a) *Step 1:* If a foreign government initiates a request for the establishment of a StanRep position with the U.S. Army, ODCSINT, HQDA will notify ODUSA(IA) and the affected MACOM or DA agency in writing and request a recommendation on the establishment of the proposed StanRep position. Such proposals will be conveyed in writing through command or agency channels. For example, if the request involves the assignment of a StanRep to a PEO PM office, ODCSINT, HQDA will send the proposal to OASA(ALT) for staffing to the appropriate PEO PM.

(b) *Step 2.* The specified DA command or agency will evaluate the proposal and submit to ODCSINT, HQDA a recommendation to approve or disapprove the proposal. If the proposal involves the assignment of a StanRep to the office of a PEO PM, the PM will coordinate his or her position with the MSC matrix support and submit the

coordinated position to OASA(ALT) which will forward the response to ODCSINT, HQDA. StanRep position proposals must provide a position description with following information, as a minimum:

1. Title of the position.
2. Position location.
3. Description of specific duties of the position.
4. Classified access level required.

5. Draft DDL or equivalent document containing data elements of a DDL. Note: According to DODD 5230.20, an equivalent document containing data elements of a DDL is required for positions necessitating access to only unclassified information. The local commander may approve this document with a copy furnished to ODCSINT, HQDA.

6. Clearly demonstrate or anticipate a mutual need for the position. The rationale must clearly demonstrate the requirement for the StanRep's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve the best interests of the U.S. Army.

(c) *Step 3.* ODCSINT, HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: ODUSA(IA), OASA (ALT), ODCSOPS, OTJAG, and the subject matter expert, if different from the preceding offices.

(d) *Step 4.* After HQDA coordination is completed, ODCSINT, HQDA will finalize the decision on the proposal and formally notify the appropriate foreign government embassy. If the proposal is approved, the DA command or agency to which the StanRep will be assigned will immediately begin to finalize the position DDL for approval and issuance by ODCSINT, HQDA. Upon receipt of the final draft DDL proposal, ODCSINT, HQDA will staff the final draft DDL with the HQDA offices cited in Step 3 (above) and other appropriate agencies. Upon concurrence and approval of the DDL, ODCSINT, HQDA, will notify the hosting Army command or agency and the appropriate foreign military attaché. The approved DDL will be in place prior to the submission of the EVA request by the appropriate foreign military attaché. Note: In the event the parent government requests that a StanRep be also certified as a FLO for security assistance matters, the above procedures will apply for the establishment of a security assistance FLO position.

(2) Request Initiated by a DA Command or Agency for Establishment of a StanRep Position.

(a) *Step 1.* Prior to beginning discussions with foreign representatives on the establishment of a StanRep position, DA commands or agencies (including PEO PMs) must obtain ODCSINT, HQDA permission to proceed. Such proposals will be conveyed in writing through command or agency channels to ODCSINT, HQDA. Proposals conveyed through PEO PMs will be sent to OASA(ALT) for forwarding to ODCSINT, HQDA.

(b) *Step 2.* A DA command or agency will provide the following information in support of its initiative to establish a StanRep position:

1. Title of the position.
2. Position location.
3. Description of specific duties of the position.
4. Classified access level required.

5. Draft DDL or equivalent document containing data elements of a DDL. Note: According to DODD 5230.20, an equivalent document containing data elements of a DDL is required for positions necessitating access to only unclassified information. The local commander may approve this document with a copy furnished to ODCSINT, HQDA.

6. The rationale must clearly demonstrate the requirement for the StanRep's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve best interests of the U.S. Army.

(c) *Step 3.* ODCSINT, HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: ODUSA(IA), OASA (ALT), ODCSOPS, OTJAG, and the subject matter expert, if different from the preceding offices.

(d) *Step 4.* After HQDA coordination is completed, ODCSINT, HQDA will finalize the decision on the initiative and formally submit the proposal to the appropriate foreign government embassy. If the latter is receptive to the proposal, ODCSINT, HQDA will direct the negotiations for DA. While the negotiations are being conducted, the DA command or agency that initiated the proposal will immediately begin to finalize the draft position DDL for approval and issuance by ODCSINT, HQDA. Upon receipt of the final draft DDL, ODCSINT, HQDA will staff the document with the HQDA offices cited in Step 3 (above) and other appropriate agencies. Upon concurrence and approval of the DDL, ODCSINT, HQDA will hold the document, awaiting conclusion of the negotiations and agreement to establish a StanRep position. Upon establishment of the StanRep position, the approved DDL will already be in place awaiting the submission of the EVA request by the appropriate foreign military attaché.

b. *Processing of StanRep Nominations.* If the StanRep position is established, ODCSINT, HQDA will process the assignment of the StanRep to a DA command or agency (see fig K-4) in the following manner:

(1) *Step 1.* The appropriate foreign military attaché will submit an EVA request at least 45 days prior to the

requested date of arrival/assignment of the StanRep. In the EVA request, the foreign military attaché provides written notification to ODCSINT, HQDA of the following—

(a) Subject individual is an officially sponsored representative of that government.
(b) Such official is authorized by the sponsoring government to conduct business with DA for purposes that must be specific.

(c) The official's legal status (including any privileges and immunities to which the individual is entitled).

(d) The official holds a specified level of security clearance.

(e) The official may assume temporary custody of CMI documentary information for courier purposes.

(f) The parent government will assume the responsibility for any and all U.S. CMI provided to the StanRep.

(2) *Step 2.* ODCSINT, HQDA will process the EVA request to the DA command or agency (PEO PM through its matrix support), to which the StanRep is to be assigned. Since the position DDL outlining the terms of the certification of the StanRep was pre-coordinated and approved, the recipient DA command or agency should respond favorably within 20 working days of the receipt of the EVA request. The DDL will remain valid until there is a change to the scope of the duties or the position is terminated. See appendix E for detailed information on DDLs.

(3) *Step 3.* Upon receipt of the concurrence of the recipient DA command or agency (PEO PM through its matrix support), ODCSINT, HQDA will approve the EVA request and notify the recipient DA command or agency of the approval. The foreign military attaché will then coordinate with the recipient DA command or agency for the arrival of the StanRep. Note: DA commands or agencies may not accept a StanRep until the DDL and visit request have been approved. If a StanRep arrives prior to visit approval, the DA command or agency involved will not permit the StanRep to commence his or her duties. The DA command or agency FDO must be notified immediately. The DA command or agency FDO will then notify the ODCSINT, HQDA, who will coordinate the disposition of StanRep with the appropriate foreign military attaché and provide instructions to the DA command or agency FDO.

c. Modification of a StanRep Position. Any proposal to change the scope of a StanRep's certification will be according to the procedures outlined in paragraphs L-4a(1) and L-4a(2), with emphasis on the specific modification. Any proposal to extend the StanRep's duration must be initiated and requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

d. Reevaluation of a StanRep Position. Once established, each StanRep position and the associated DDL will be reevaluated on each successive nomination to ensure that the best interests of the host command or agency and DA continue to be served, and the purpose of the position remains valid. To alleviate the possibility of a StanRep arriving to assume an established position prior to visit approval, ODCSINT, HQDA will initiate contact with the appropriate foreign government Military Attaché in Washington, DC, 90 days prior to the tour expiration date of the incumbent StanRep and query the foreign military attaché concerning a replacement for the position, extension of the incumbent StanRep, or other alternatives contemplated by the parent government. The ODCSINT, HQDA will also inform the sponsoring Army command or agency of the intended action, if any, of the foreign government to alter the status of the StanRep position. The host command or agency FDO and contact officer will also commence their reevaluation 90 days prior to the tour expiration date of the incumbent StanRep.

L-5. Administering StanReps

a. Visits.

(1) It should be noted that the foreign government StanReps need not coordinate their attendance at formalized ABCA meetings (that is, QWG, DA-hosted/sponsored meeting, etc.) with their respective contact officers.

(a) However, foreign government StanReps must coordinate arrangements for all non-formalized ABCA meeting (that is, a meeting not hosted by a U.S. Army member or attended by all members of the group, etc.) visits with their respective contact officers.

(b) To support all formalized and non-formalized ABCA meetings, ODUSA(IA) and ODCSINT, HQDA will be responsible for the following—

1. ODUSA(IA) will ensure that the current StanList accurately reflects the subjects over which the U.S. Army has responsibility and is disseminated to all affected commands and agencies, to include weapons system PMs, subject matter experts, responsible FDOs, etc.

2. ODCSINT, HQDA will ensure that proper disclosure guidance is provided to all affected commands and agencies, to include weapons system PMs, subject matter experts, responsible FDOs, etc.

(2) Visits (exclusive of formalized ABCA meetings) by StanReps may be approved by the contact officer if the proposed destination is within the organizational jurisdiction of DA and the purpose of the visit is within the scope of the StanRep's approved terms of certification. The contact officer is required to coordinate such visits between activities and do not require official authorization from ODCSINT, HQDA.

(3) All visits by StanReps to destinations outside the terms of certification must be initiated on the StanRep's behalf by their military attaché through the FVS.

(4) All visits by StanReps to destinations outside DA jurisdiction (that is, destinations under the organizational

jurisdiction of other services, OSD, JCS - including unified and specified commands - and other Federal departments and agencies) but within the terms of certification will be coordinated by the StanRep's contact officer. The contact officer will comply with the procedures of the intended recipient organization for the visit. For example, the intended recipient organization may require a letter of request from the StanRep's parent embassy. In such cases, the contact officer should have the StanRep notify his or her embassy of the intended recipient organization's requirements and obtain the proper documentation for submission to the intended recipient organization.

(5) Travel-related funding for all StanRep visits will be according to the Basic Standardization Agreement of 1964.

b. Library and publications support. At the discretion of the host activity's contact officer, a StanRep may be granted supervised access to unclassified (CUI included) sections of activity libraries. Additionally, each StanRep may be provided a reference set of DA and activity publications necessary to the successful performance of the StanRep's duties, consistent with the StanRep's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the StanRep's successor when the StanRep's certification ends.

c. Computer access. StanReps may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is authorized for disclosure to their government. See paragraph L-2g for information regarding e-mail addresses and messages. The use of personal computers by StanReps may be permitted, provided proper authorization is granted. In all cases, the provisions of AR 380-19 and local security procedures will apply.

d. Misconduct. StanReps serve at the pleasure of DA and must conform to the Army's customs and traditions and comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If a StanRep violates the terms of certification, violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the contact officer will notify the local agency or command FDO and provide a written report on the inappropriate action, through command channels, to ODCSINT, HQDA, with a recommendation for final disposition by HQDA, such as temporary suspension or permanent revocation of privileges, or revocation of certification. ODCSINT, HQDA will coordinate the resolution of all cases involving StanRep misconduct.

L-6. U.S. contact officer

a. Contact officers will be designated in writing by the commander or agency head, or their designees to facilitate and oversee the activities of StanReps at DA commands or agencies. The contact officer should be of equivalent rank/grade or higher, if available, to the StanRep. A primary and an alternate contact officer must be identified in the DDL (para 8). They must be physically accessible to and have daily contact with the StanRep. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his or her duties. Contact officers will also adhere to the guidelines listed below. Note: In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the U.S. Army.

b. The contact officer for a StanRep will-

(1) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by ODCSINT, HQDA for the individual StanRep position.

(2) Initially brief a new StanRep on DA and local policies and procedures affecting the StanRep's status and performance of functions, as well as customs of the U.S. Army; subsequently, the contact officer will render advice and assistance to the StanRep in complying with such policies and procedures. The contact officer will have the StanRep sign a statement, similar to the document exhibited at figure L-2, indicating his or her agreement and understanding. The contact officer will provide a copy of the signed certification form to the StanRep.

(3) In conjunction with the FDO, evaluate the StanRep's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the StanRep's approved terms of certification. Consultations and visits beyond a StanRep's terms of certification require the submission of formal visit requests by the StanRep's embassy in Washington, D.C.

(4) Receive, evaluate, and recommend/refer all StanRep requests for CMI to the FDO.

(5) Receive, evaluate, and refer all StanRep requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent, who will render a disclosure decision and return the action to the FDO for case closure.

(6) Notify the ODCSINT, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of StanReps under their oversight.

(7) Notify the supporting counterintelligence and local security offices of any foreign visitor activity which is reportable under the provisions of AR 381-12.

(8) Comply with the procedures cited in paragraph L-5d of this appendix regarding misconduct on the part of the StanRep.

(9) Brief U.S. personnel with whom the StanRep will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

USASAC will ensure that the following standardized conditions and limitations are entered into the LOA for StanReps, not otherwise covered by a MOA.

1. The StanRep will represent the Parent Party to the Host Party. The StanRep will not perform duties reserved by the laws or regulations of the Host Government to officers or employees of the Host Government, nor will the StanRep provide any labor or services to the Host Government or any of its agencies, including the Host Party.

2. The StanRep will comply with all applicable Host Country policies, procedures, laws and regulations. The Host Party will assign a Contact Officer to provide guidance to the StanRep concerning requirements of the Host Party and to arrange for activities consistent with such requirements and the purposes of this LOA.

3. The StanRep may request access to Host Party facilities if such access promotes the purposes of this LOA, is consistent with the terms of any applicable formal certification or approval issued by the Host Country, and is permitted under the applicable laws and regulations of the Host Country. Such requests will be submitted to the Contact Officer. Approval of such requests will be at the discretion of the Host Country. Any request for access that exceeds the terms of an applicable certification or approval will be submitted through diplomatic channels.

4. The StanRep will not be granted access to information of the Host Party, whether or not classified, except as authorized by the Host Party, and only to the extent necessary to fulfill the StanRep's functions herein.

5. All information to which the StanRep is granted access while serving as a liaison to the Host Party will be treated as information provided to the Parent Government, in confidence, and will not be further released or disclosed by the StanRep to any other person, firm, organization, or government without the prior written authorization of the Host Government. Disclosure of information to the StanRep will not be deemed to be a license or authorization to use such information for any purpose other than the purposes described herein.

6. The StanRep will not be assigned to locations where hostilities are likely. Should hostilities occur at a location where the StanRep is assigned, the Host Party will promptly remove the StanRep to a location where involvement by the StanRep in such hostilities is unlikely.

7. The StanRep will not participate in exercises or civil-military actions, unless expressly authorized to do so by both the Host and Parent Party.

Figure L-1. StanRep LOA conditions and limitations

8. The StanRep will comply with the dress regulations of the Parent Party, but, if requested by the Host Party, will also wear such identification as may be necessary to identify the StanRep's nationality, rank and status as a StanRep. The order of dress for any occasion will be that which most closely conforms to the order of dress for the particular unit of the Host Party, which the StanRep is serving. The StanRep will comply with the customs of the Host Party with respect to the wear of civilian clothing.

9. Prior to the commencement of a StanRep's tour, the Parent Party will notify the Host Party of the specific Parent Party organization which will exercise operational control over the StanRep and, if different, the Parent Party organization that will provide administrative support to the StanRep and the StanRep's dependents.

10. At the end of a StanRep's tour, or as otherwise agreed by the Parties, the Parent Party may replace the StanRep with another individual who meets the requirements of this LOA. Such replacement will be subject to any certification or approval requirements imposed under the laws and regulations of the Host Party.

11. The Host Party's certification or approval of an individual as a StanRep will not, in and of itself, bestow diplomatic or other special privileges on that individual.

12. The Host Party will establish the maximum substantive scope and classification levels within which the disclosure of any Classified Information or Controlled Unclassified Information to the StanRep will be permitted. The Host Party will inform the Parent Party of the level of security clearance required to permit the StanRep access to such information.

13. Each Party will cause security assurances to be filed stating the security clearances for the StanRep being assigned by such Party. The security assurances will be prepared and forwarded through prescribed channels in compliance with established Host Party procedures.

14. The Parent Party will ensure that each assigned StanRep is fully cognizant of, and complies with, applicable laws and regulations concerning the protection of proprietary information (such as patents, copyrights, know-how, and trade secrets), classified information and controlled unclassified information disclosed to the StanRep. This obligation will apply both during and after termination of an

Figure L-1. StanRep LOA conditions and limitations—Continued

assignment as a StanRep. Prior to taking up duties as a StanRep, the StanRep will be required to sign the certification form. Only individuals who execute the certification form will be permitted to serve as StanReps.

15. The Parent Party will ensure that the StanRep, at all times, complies with the security laws, regulations and procedures of the Host Government. Any violation of security procedures by a StanRep during his or her assignment will be reported to the Parent Party for appropriate action. Upon request by the Host Party, the Parent Party will remove any StanRep who violates security laws, regulations, or procedures during his or her assignment, or fails to display a commitment to comply with such laws, rules, or procedures.

16. All classified information made available to the StanRep will be considered to be classified information furnished to the Parent Party, and will be subject to all provisions and safeguards provided for under the General Security of Military Information Agreement (GSOMIA) or equivalent security arrangement.

17. The StanRep will not take custody of classified information or controlled unclassified information in tangible form (for example, documents or electronic files), except to act as a courier and as expressly permitted by the terms of the formal certification or approval of the StanRep and as authorized by the Parent Government.

18. The obligations of the StanRep and the Parent Party with respect to classified or controlled unclassified information disclosed by the Host Party in connection with this Agreement will survive termination or expiration of this LOA.

19. Consistent with the laws and regulations of the Host Government and this Agreement, the StanRep will be subject to the same restrictions, conditions, and privileges as Host Party personnel of comparable rank and in comparable assignments. Nothing herein will limit any exemption from taxes, customs or import duties, or similar charges available to the StanRep or the StanRep's dependents under applicable laws and regulations or any international agreement between the Host Government and the Parent Government.

20. Unless otherwise agreed by the Parties, the StanRep will reside within commuting distance from the Host Party unit or office with which the StanRep is serving as a liaison.

21. Neither the Host Party nor the armed forces of the Host Government may take disciplinary action against a StanRep who commits an offense under the military laws or regulations of the Host Party, nor will the Host Party exercise disciplinary authority over the StanRep's dependents. The Parent Party, however, will take such administrative or disciplinary action against the StanRep,

Figure L-1. StanRep LOA conditions and limitations—Continued

as may be appropriate under the circumstances, to ensure compliance with this Agreement, and the Parties will cooperate in the investigation of any offenses under the laws or regulations of either Party.

22. The certification or approval of a StanRep may be withdrawn, modified or curtailed at any time by the Host Party for any reason, including, but not limited to, the violation of the regulations or laws of the Host Party or the Host Government. In addition, at the request of the Host Party, the Parent Government will remove the StanRep or a dependent of the StanRep from the territory of the Host Country. The Host Party will provide an explanation for its removal request, but a disagreement between the Parties concerning the sufficiency of the Host Party's reasons will not be grounds to delay the removal of the StanRep or his/her dependent. If so requested by the Host Party, the Parent Party will replace any StanRep removed under this Paragraph, provided the replacement meets the requirements of this LOA.

23. A StanRep will not exercise disciplinary or supervisory authority over military or civilian personnel of the Host Party.

Figure L-1. StanRep LOA conditions and limitations—Continued

[Office Symbol]

[Date]

SECTION I

STANREP

LEGAL STATUS OF CERTIFICATION

As a representative of the [foreign organization] under the auspices of an Extended Visit Authorization to the [DOD Service, agency or organization], I am subject to the jurisdiction of United States federal, state, and local laws, except as provided by treaty, other specific legal authority, or the terms of any diplomatic immunity which I may have been granted. I understand that my acceptance of the StanRep position does not bestow diplomatic or other special privileges.

SECTION II

STANREP

CONDITIONS OF CERTIFICATION

(1) Responsibilities: I understand that my activities will be limited to the representational responsibilities of my government and that I am expected to present the views of my government with regard to the issues which my

Figure L-2. Sample certification

government and the U.S. Government have a mutual interest. I will not perform duties that are reserved by law or regulation to an officer or employee of the U.S. Government.

(2) **Costs:** I understand that all costs associated with my duties as a StanRep will be the responsibility of my government, including, but not limited to, travel, office space, clerical services, quarters, rations, and medical and dental services.

(3) **Extensions and Revalidation:** I understand that if my government desires to request an extension or revalidation of my position beyond the original dates for which I am certified, a new visit request will be submitted not later than 30 days prior to the expiration date of the current Extended Visit Authorization.

(4) **Contact Officer:** I understand that when the certification process is completed, a contact Officer(s) will be assigned to sponsor me during my visit to the [DOD Service, agency or organization]. I further understand that I will coordinate, through my Contact Officer, all requests for information, visits, and other business, which fall under the terms of my certification. I also understand that requests for information, which are beyond the terms of my certification, will be made through the Office of the Defense Attaché.

Figure L-2. Sample certification—Continued

(5) Other Visits: I understand that visits to facilities for which the purpose does not directly relate to the terms of my certification will be made through the Office of the Defense Attaché.

(6) Uniform: I understand that I will wear my national uniform or appropriate civilian attire when conducting business at the [location of the United States Government facility] or other Department of Defense facilities, unless otherwise directed. I will comply with my Parent Government's service uniform regulations.

(7) Duty Hours: I understand that my duty hours are Monday through Friday, from (TIME) to (TIME). Should I require access to my work area during non-duty hours, I am required to request permission from the Command Security Officer. I further understand that (IT IS) (IT IS NOT) necessary to assign a United States escort officer to me during my non-duty access. Any cost incurred as a result of such non-duty access may be reimbursable to the United States Government.

(8) Security:

a. I understand that access to U.S. Government information will be limited to that information determined by my Contact Officer to be necessary to fulfill the functions of a StanRep. I also understand that I may not have unsupervised access to U.S. Government computer systems, unless the information accessible

Figure L-2. Sample certification—Continued

by the computer is releasable to my government according to applicable U.S. law, regulations and policy.

b. All information to which I may have access during my certification will be treated as information provided to my government in confidence and will not be further disclosed or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the United States Government.

c. I understand that all Classified Material (United States or Parent Government) is to remain under the control of the Host Party and is subject to inspection by Host Party security officials. This does not preclude issuance of a security container for temporary storage of Classified Information if justification exists and is consistent with the terms of my certification. The Host Party supplied container and its contents will remain the responsibility of the Host Party, to include the security combination.

d. While assigned to (U.S. Army Organization), I will comply with all United States Army administrative rules and security regulations. I understand that my office is subject to safety and security inspections.

Figure L-2. Sample certification—Continued

e. I may not reproduce U.S. Classified Information for which I have assumed temporary custody. I am authorized to reproduce controlled unclassified information.

f. I will immediately report to both my Contact Officer should I obtain or become knowledgeable of United States Government information for which I am not authorized to have access. I further agree that I will report to my Contact Officer any incidents of my being offered or provided information that I am not authorized to have.

g. If required, I will display a security badge on my outer clothing so that it is clearly visible. The United States Government will supply this badge.

(9) Compliance: I have been briefed on, fully understand, and will comply with the terms and conditions of my certification. Failure to comply may result in termination of my certification. I further understand that the termination of my certification does not preclude further disciplinary action according to any applicable Status of Forces Agreement or other government-to-government agreements.

Figure L-2. Sample certification—Continued

(10) Terms. Terms not defined herein will have the definitions ascribed to them in the applicable Agreement governing my assignment as a StanRep.

SECTION III
STANREP
TERMS OF CERTIFICATION

(1) Contact officer: (NAME OF CONTACT OFFICER[s]) has been assigned as my Contact officer.

(2) Certification: I am certified to the [DOD Service, agency or organization] in support of the following programs/topics/etc.

(3) Travel: I may visit the following locations under the terms of my certification, with the permission of my Contact officer:

SECTION IV
STANREP
CERTIFICATION OF IN-BRIEFING

I, (NAME OF STANREP), understand and acknowledge that I have been certified as a StanRep to the [DOD Service, agency or organization], as agreed

Figure L-2. Sample certification—Continued

upon between the [foreign organization] and the United States [DOD Service, agency or organization]. I further acknowledge that I fully understand and have been briefed on: (1) the legal status of my certification; (2) the conditions of my certification; and (3) the terms of my certification. I further acknowledge that I will comply with the conditions and responsibilities of my certification.

SIGNATURE OF STANREP

DATE

TYPED NAME OF STANREP

SIGNATURE OF BRIEFER

RANK AND OR TITLE

TYPED NAME

Figure L-2. Sample certification—Continued

Appendix M Military Personnel Exchange Program

M-1. Concept

The Military Personnel Exchange Program (MPEP) with armies of other Nations involves the assignment of U.S. Army and foreign armed forces personnel to authorized positions within each party's military establishment. ODCSOPS, HQDA (DAMO-SSF) is the proponent for the program and directs it under the provisions of AR 614-10. MPEP is designed to foster mutual understanding between the military establishments of each party by providing exchange personnel familiarity with the organization, administration, and operations of the host military establishment. According to applicable exchange program regulations, foreign military personnel are integrated into the DA work force. Such exchanges are established under a formal MOA between the U.S. Army and a foreign military service under AR 550-51. Unilateral assignment of foreign officers to U.S. positions without reciprocity violates statutory prohibitions against the acceptance of voluntary services by an agency of the Federal Government. Likewise, the unilateral assignment of U.S. officers to foreign positions, absent reciprocity, may constitute the provision of unauthorized security assistance to such countries.

M-2. Conditions and Limitations

- a. MPEP participants will not act in the dual capacity as a foreign exchange personnel participant and as a representative of their government (for example, a FLO) while assigned to a DA command.
- b. MPEP participants will not serve as conduits between DA and their government for requests and transmission of

CMI and CUI nor be used as a mechanism for exchanging technical data or other controlled information between the governments.

c. Foreign MPEP participants will not be assigned to command or other positions that would require them to exercise responsibilities reserved by law or regulation to an officer or employee of the USG. They will not, for example, perform responsibilities of a contracting officer's technical representative, component duty officer, classified document custodian or security officer, escort for foreign visitors, or perform other official acts as a representative of DA.

d. MPEP participants will not be assigned to DOD contractor facilities.

e. DA will not submit ENDP requests solely to accommodate the establishment of a MPEP position.

f. The assignment of MPEP participants will not be used for training foreign personnel in violation of DOD 5105.38M or, instead of, or in combination with MPEP certification. Pursuant to Section 1082 of Public Law 104-201, training may not be conducted under the MPEP except as necessary to familiarize, orient, or certify MPEP participants regarding unique aspects of the positions to which they are assigned.

g. MPEP participants will not be used for the purpose of augmenting DA staff positions or as a means to obtain personnel resources beyond authorized manning levels.

h. MPEP participants will not be placed in duty positions that could result in their access to CMI or CUI that has not been authorized for disclosure to their government.

i. MPEP participants will not have permanent custody of CMI and CUI. They may have access to the information during normal duty hours at the place of assignment when access is necessary to perform their duties and the information is authorized for disclosure pursuant to the DDL or equivalent disclosure guidance. In all cases, local security policies and procedures apply.

j. MPEP participants' access to restricted areas will be according to AR 190-13 and local security policies and procedures and as specified in DDLs or equivalent disclosure guidance documents.

k. MPEP participants will wear their uniforms according to local command customs and tradition. If required, they will wear, in clear view, a DA building or installation pass or badge that clearly identifies them as foreign nationals.

l. Any other identification (including organizational code and title, block, office nameplate, security badge, or e-mail address) used by or issued to MPEP participants by the host Army units will clearly identify the MPEP participant's status as a foreign national. For example, an e-mail address will resemble the following: "SmithJ(full country name National)@hqda.army. mil". Acronyms for country names will not be used. The recipient of the MPEP's e-mail message must be able to identify the MPEP as a foreign national.

M-3. MPEP MOA and Certification

a. *MOA.* AR 614-10 provides detailed information on MPEP MOAs.

b. *Certification.*

(1) MPEP participants are certified to DA commands or agencies to perform assigned duties. Terms of certification are derived from and are consistent with the scope of the MOA.

(2) Each MPEP participant must sign a certification statement acknowledging the terms of his or her assignment (see fig M-1). A copy of the signed certification statement, which will be maintained by the local FDO, must be provided to the MPEP and ODCSOPS, HQDA (DAMO-SSF) (within 15 days of signature). If the MPEP participant refuses to sign the certification statement, the command or agency must immediately notify ODCSINT, HQDA, which will notify the DA proponent and together resolve the issue through the parent government's military attaché in Washington, DC.

M-4. Establishment of MPEP Positions and Processing of MPEP Nominations.

a. *Establishment of MPEP Positions.* Only the HQDA proponent may approve establishment, dis-establishment, or changes to MPEP positions (see fig M-2). A DDL or equivalent disclosure guidance is required for all MPEP positions.

b. *Processing of MPEP Nominations.* All MPEP nominations will be processed (see fig K-4) in the following manner:

(1) Step 1: The appropriate foreign military attaché will submit an EVA request at least 45 days prior to the requested date of assignment of the MPEP participant. In the EVA request, the foreign military attaché provides written notification to ODCSINT, HQDA of the following—

(a) Subject individual is an officially-sponsored exchange participant of that government.

(b) The official holds a specified level of security clearance.

(c) The parent government will assume the responsibility for any and all U.S. CMI provided to the MPEP participant.

(2) Step 2: ODCSINT, HQDA will process the EVA request to the command or agency to which the MPEP participant is to be assigned. Since the position DDL or equivalent disclosure guidance outlining the terms of the certification of the MPEP participant will be pre-coordinated and approved, the recipient DA command or agency should respond favorably within 20 working days of the receipt of the EVA request. The position DDL or equivalent

disclosure guidance will remain valid until there is a change to the scope of the position or the position is terminated. See appendix E for detailed information on DDLs.

(3) Step 3: Upon receipt of the concurrence of the recipient command or agency, ODCSINT, HQDA will approve the EVA request and notify ODCSOPS, HQDA, the foreign military attaché, and the recipient command or agency of the approval. The foreign military attaché will then coordinate with the recipient command or agency for the arrival of the MPEP participant. Note: DA commands or agencies may not accept a MPEP participant until the DDL and visit request have been approved. If MPEP participant arrives prior to visit approval, the command or agency involved will not permit the MPEP participant to commence his or her duties. The command or agency FDO must be notified immediately. The command or agency FDO will then notify ODCSINT, HQDA, who will coordinate the disposition of MPEP participant with ODCSOPS, HQDA and the appropriate foreign military attaché and provide instructions to the command or agency FDO.

c. Modification of a MPEP Position. Any proposal to change the scope of a MPEP participant's certification will be according to the procedures outlined in AR 614-10, with emphasis on the specific modification. ODCSOPS, HQDA (DAMO-SSF) will effect the necessary coordination (that is, modifications to an existing DDL or equivalent disclosure guidance, if required) to render a decision regarding the request. Any proposal to extend the MPEP participant's duration must be initiated and requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

d. Reevaluation of a MPEP Position. Once established, each MPEP position and the associated position DDL will be reevaluated on each successive nomination to ensure that the best interests of the host element and DA continue to be served, and the purpose of the position remains valid.

M-5. Administering MPEP Participants

a. Visits. All visits or travel by the MPEP participant will be according to the standing operating procedures of the unit of assignment. However, all travel orders will identify the individual as a MPEP participant assigned to the U.S. Army. ODCSOPS, HQDA approval is required for all OCONUS travel by any MPEP participant.

b. Library and publications support. At the discretion of the host activity's contact officer and through coordination with the FDO, a MPEP may be granted supervised access to the CMI section of the command or agency library. Additionally, each MPEP may be provided a reference set of DA and activity publications necessary to the successful performance of the MPEP's duties, consistent with the MPEP's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the MPEP's successor when the MPEP's certification ends.

c. Computer access. MPEPs may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is authorized for disclosure to their government. See paragraph M-2I for information regarding e-mail addresses and messages. In all cases, the provisions of AR 380-19 and local security procedures will apply.

d. Misconduct. MPEPs serve at the pleasure of DA and must conform to the Army's customs and traditions and comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If a MPEP violates the terms of certification, violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the contact officer will notify the local agency or command FDO and provide a written report on the inappropriate action, through command channels, to ODCSOPS, HQDA (DAMO-SSF), with a recommendation for final disposition, such as temporary suspension or permanent revocation of privileges, or revocation of certification. ODCSOPS, HQDA (DAMO-SSF) will provide a copy of the report to ODCSINT, HQDA, and ODUSA(IA), and coordinate the resolution of all MPEP misconduct cases.

M-6. Supervisor Functions

DA officials designated to supervise a MPEP participant will —

- a.* Ensure that the MPEP participant understand the duties to be performed in the assigned position.
- b.* Ensure that the MPEP participant is provided access only to that CMI and CUI necessary to fulfill the duties of the position description as described in the DDL or equivalent disclosure guidance.
- c.* Be familiar with this regulation, other applicable regulatory guidance governing the disclosure of CUI, and specific disclosure guidelines established in the DDL or equivalent disclosure guidance.
- d.* Inform co-workers of the disclosure limitations on access to CMI and CUI related to the MPEP participant and their responsibilities in dealing with the MPEP participant.
- e.* Ensure that the MPEP participant signs a certification similar to the sample in figure M-1 before being assigned to the position.

M-7. U.S. contact officer

a. Contact officers will be designated in writing by commanders or agency heads, or their designees to facilitate and oversee the activities of MPEPs at DA commands or agencies. The contact officer should be of equivalent rank/grade

or higher, if available, to the MPEP. A primary and an alternate contact officer must be identified in the DDL (para 8). They must be physically accessible to and have daily contact with the MPEP. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his or her duties. Contact officers will also adhere to the guidelines listed below. Note: In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the U.S. Army.

b. The contact officer for a MPEP will –

(1) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by ODCSINT, HQDA for the individual MPEP position.

(2) Initially brief a new MPEP on DA and local policies and procedures affecting the MPEP's status and performance of functions, as well as customs of the U.S. Army; subsequently, the contact officer will render advice and assistance to the MPEP in complying with such policies and procedures. The contact officer will have the MPEP sign a statement, similar to the document exhibited at figure M-1, indicating his or her agreement and understanding. The contact officer will provide a copy of the signed certification form to the MPEP.

(3) In conjunction with the FDO, evaluate the MPEP's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the MPEP's approved terms of certification. Consultations and visits beyond a MPEP's terms of certification require the submission of formal visit requests by the MPEP's embassy in Washington, DC.

(4) Receive, evaluate, and recommend/refer all MPEP requests for CMI to the FDO.

(5) Receive, evaluate, and refer all MPEP requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent, who will render a disclosure decision and return the action to the FDO for case closure.

(6) Notify the ODCSINT, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of MPEPs under their oversight.

(7) Notify the supporting counterintelligence and local security offices of any foreign visitor activity that is reportable under the provisions of AR 381-12.

(8) Comply with the procedures cited in paragraph M-5d of this appendix regarding misconduct on the part of the MPEP.

(9) Brief U.S. personnel with whom the MPEP will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions. The contact officer will have the MPEP participant sign a copy of the statement exhibited at figure M-1, indicating his or her agreement and understanding.

CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES
FOR FOREIGN MPEP PARTICIPANTS

I understand and acknowledge that I have been accepted for assignment to (insert name and location of organization to which assigned) pursuant to an agreement between the United States Army and the (insert applicable foreign military organization) of (insert country name). In connection with this assignment, I further understand, acknowledge, and certify that I will comply with the following conditions and responsibilities:

1. The purpose of the assignment is to gain knowledge of the organization and management of Host Party (cite applicable area for foreign exchange personnel assignment) defense activities. There will be no access to information except as required to perform the duties described in the position description of the position to which I am assigned, as determined by my designated supervisor.

2. I will perform only functions which are properly assigned to me as described in the position description (PD) for my assignment and will not act in any other capacity on behalf of my government or my Parent Party or Parent Organization.

3. All information to which I may have access during this assignment will be treated as information provided to my government in confidence and will not be further released or disclosed by me to any other person, firm, organization or government without the prior written authorization of the Host Party.

4. When dealing with individuals outside of my immediate office of assignment on official matters, I will inform such individuals that I am a foreign exchange person.

5. I have been briefed on, understand, and will comply with all applicable security regulations of the Host Party and the Host Organization.

Figure M-1. Sample certification for MPEP participant

6. I will immediately report to my designated supervisor all attempts by unauthorized persons to obtain classified, proprietary or controlled unclassified information to which I may have access as a result of this assignment.

(SIGNATURE)

(TYPED NAME)

(RANK/TITLE)

(DATE)

Figure M-1. Sample certification for MPEP participant—Continued

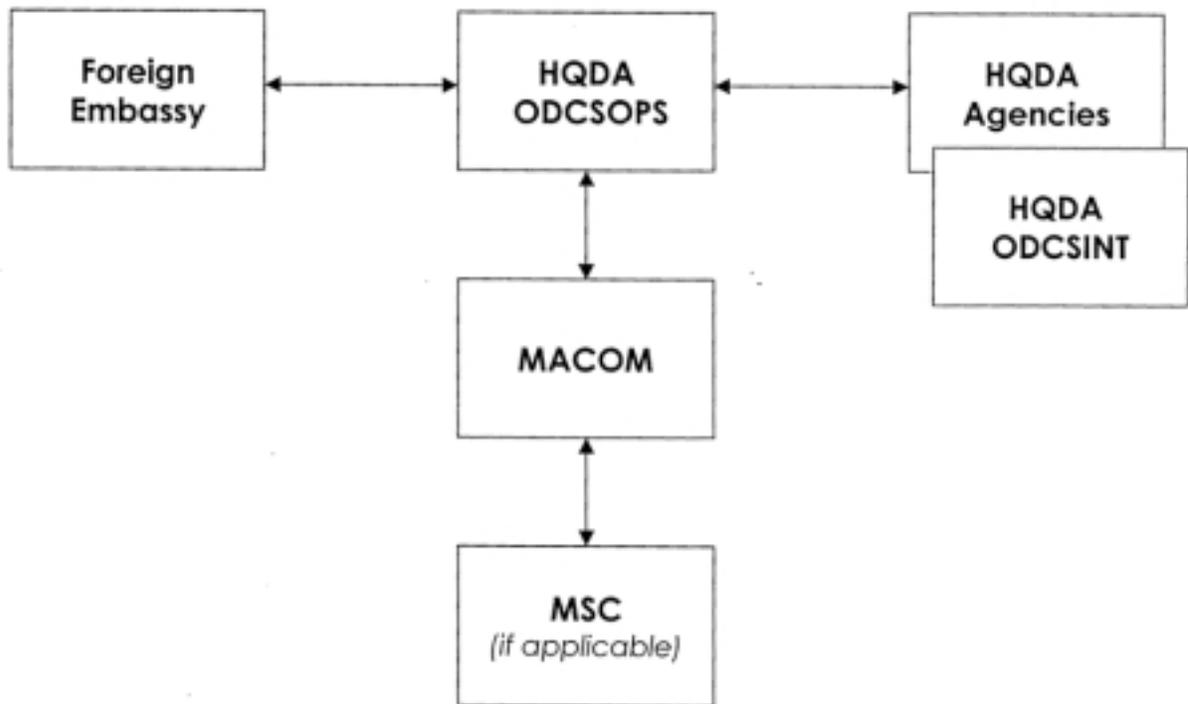


Figure M-2. Establishment of MPEP positions here

Appendix N Engineers and Scientists Exchange Program

N-1. Concept

The Engineers and Scientists Exchange Program (ESEP) is a professional development endeavor that promotes international cooperation in military research, development, test and evaluation (RDT&E) through the exchange of military and or government civilian scientists and engineers. This program provides on-site working assignments for foreign personnel in U.S. Army activities, and for U.S. personnel in foreign army activities. The work assignments will provide ESEP personnel work experience as spelled out under an approved position description and at the direction of a host supervisor, as well as knowledge of the organization and management of that army establishment to which they are assigned. HQ, AMC, exercises DA responsibility for the program. AR 70-58 and the ESEP Letter of Instruction are the governing documents. At HQDA, the ODUSA(IA) is responsible for overseeing matters pertaining to the ESEP.

a. The goals of the program are to leverage state-of-the-art technology of mutual interest to the U.S. and the foreign country involved, conserve scarce resources by reducing duplicative RDT&E efforts, and promote mutual cadres of defense professionals who will continue to support international armaments cooperation activities.

b. The ESEP is not a training program, a means of exchanging personnel for production or co-development purposes, nor a means of augmenting personnel resources above currently authorized manning levels.

N-2. Conditions and Limitations.

a. ESEP participants will not act in the dual capacity as a foreign exchange personnel participant and as a representative of their government (for example, a FLO) while assigned to a DA command or agency.

b. ESEP participants will not serve as conduits between DA and their government for requests and transmission of CMI and CUI nor be used as a mechanism for exchanging technical data or other controlled information between the governments.

c. ESEP participants will not be assigned to command or other positions that would require them to exercise responsibilities reserved by law or regulation to an officer or employee of the USG. They will not, for example, perform responsibilities of a contracting officer's technical representative, component duty officer, classified document custodian or security officer, escort for foreign visitors, or perform other official acts as a representative of DA.

d. ESEP participants will not be assigned to DOD contractor facilities.

e. DA will not submit ENDP requests solely to establish an ESEP position.

f. The assignment of ESEP participants will not be used for training foreign personnel in violation of DOD 5105.38M or, instead of, or in combination with FLO certification. Pursuant to Section 1082 of Public Law 104-201, training may not be conducted under the ESEP except as necessary to familiarize, orient, or certify ESEP participants regarding unique aspects of the positions to which they are assigned.

g. ESEP participants will not be used for the purpose of augmenting DA staff positions or as a means to obtain personnel resources beyond authorized manning levels.

h. ESEP participants will not be placed in duty positions that could result in their access to CMI or CUI that has not been authorized for disclosure to their government.

i. ESEP participants may have temporary custody of CMI and CUI necessary to perform their duties and the information is authorized for disclosure pursuant to the DDL or equivalent disclosure guidance. In all cases, local security policies and procedures apply.

j. ESEP participants' access to restricted areas will be according to AR 190-13 and local security policies and procedures and as specified in DDLs or equivalent disclosure guidance documents.

k. ESEP military participants will wear their uniforms while civilian participants will wear civilian attire according to local command customs and tradition. They will wear, in clear view, a DA building or installation pass or badge (if required) that clearly identifies them as foreign nationals.

l. Any other identification (including organizational code and title, block, office nameplate, security badge, or e-mail address) used by or issued to ESEP participants by the host Army units will clearly identify the ESEP participant's status as a foreign national. For example, an e-mail address will resemble the following: "SmithJ(full country name National)@hqda.army.mil". Acronyms for country names will not be used. The recipient of the ESEP's e-mail message must be able to identify the ESEP as a foreign national.

m. ESEP participants will sign a statement regarding invention rights (see fig N-1).

N-3. ESEP MOU and Certification

a. *MOU.* AR 70-58 provides the overarching authority for the ESEP, and the DOD-State Department certified, model "ESEP MOU" details the content of an ESEP MOU.

b. *Certification.*

(1) ESEP participants are certified to a DA activity to perform duties of his or her position description under the auspices of an "Approval to Place Agreement," Certificate of Conditions and Responsibilities (see fig N-2), Commitment Regarding Inventions Made and Technical Information Developed by Visiting Engineers and Scientists per the DA ESEP Letter of Instruction and an EVA. These terms of certification are derived from and are consistent with the scope of existing bilateral ESEP international agreements.

(2) Each ESEP participant must sign the aforementioned Certificate of Conditions and Responsibilities acknowledging the terms of his or her assignment. The ESEP participant will be provided a copy of the signed certification during the approval process. If the ESEP participant refuses to sign the certification statement, the command or agency must immediately notify ODCSINT, HQDA, which will notify the DA proponent and HQ, AMC, and together resolve the issue with the parent government's military attaché in Washington, DC.

N-4. Establishment of ESEP Positions and Processing of ESEP Nominations.

a. *Establishment of ESEP Positions.* Only HQ, AMC may approve the establishment of ESEP positions (see fig N-3). HQ, AMC is responsible for coordinating prospective ESEP positions with the relevant host placement activity level, MACOM level and DA level entities. Note: Within HQDA, AMC will coordinate ESEP actions with the following offices (at a minimum): OASA(ALT), ODCSINT, ODCSOPS, and the Office of the General Counsel. The following ESEP establishment procedures are as follows:

(1) HQ, AMC will forward the nomination to the Army host activity, which will examine the nomination to ensure that the nominee is qualified for the proposed position.

(2) The host activity must ensure that the entire ESEP nomination package (that is, Approval to Place Agreement

(without signatures), Resume, Career Areas of Interest, Certificate of Conditions and Responsibilities (without signature), Commitment Regarding Inventions Made and Technical Information Developed (without signature) and DDL or equivalent disclosure guidance is completed NLT 60 days following receipt of the nomination.

(3) Upon receipt of the nomination package from the host activity, HQ, AMC, will coordinate the nomination package, and execute internal and HQDA coordination to approve the nomination.

(4) Upon internal review and approval, HQ, AMC, will sign the Approval to Place Agreement and forward it to country for foreign ESEP Executive Agent signature, and nominee signature of the Certificate of Conditions and Responsibilities and Commitment Regarding Inventions Made and Technical Information Developed.

(5) Upon receipt of the above documentation, HQ, AMC, will notify the nominee's Embassy to submit the EVA.

b. Processing of ESEP Nominations. The procedures for processing ESEP nominations (see fig N-4) can be found in the ESEP/ESEP Letter of Instruction. In summary, upon receipt of the foreign government nomination:

(1) *Step 1:* The appropriate foreign military attaché will submit an EVA request at least 45 days prior to the requested date of assignment of the ESEP participant. In the EVA request, the foreign military attaché provides written notification to ODCSINT, HQDA of the following:

(a) Subject individual is an officially-sponsored exchange participant of that government.

(b) The official holds a specified level of security clearance.

(c) The parent government will assume the responsibility for any and all U.S. CMI provided to the ESEP participant.

(2) *Step 2:* ODCSINT, HQDA will process the EVA request to the command or agency to which the ESEP participant is to be assigned. Since the position DDL or equivalent disclosure guidance outlining the terms of the certification of the ESEP participant will be pre-coordinated and approved, the recipient DA command or agency will respond favorably within 20 working days of the receipt of the EVA request. The position DDL or equivalent disclosure guidance will remain valid until there is a change to the scope of the position or the position is terminated. See appendix E for detailed information on DDLs.

(3) *Step 3:* Upon receipt of the concurrence of the recipient command or agency, ODCSINT, HQDA will approve the EVA request and notify ODUSA(IA), HQ, AMC, the foreign military attaché, and the recipient command or agency of the approval. The foreign military attaché will then coordinate with the recipient command or agency for the arrival of the ESEP participant. Note: DA commands or agencies may not accept a ESEP participant until the DDL and visit request have been approved. If ESEP participant arrives prior to visit approval, the command or agency involved will not permit the ESEP participant to commence his or her duties. The command or agency FDO must be notified immediately. The command or agency FDO will then notify ODCSINT, HQDA, who will coordinate the disposition of ESEP participant with ODUSA, HQDA, HQ, AMC, and the appropriate foreign military attaché and provide instructions to the command or agency FDO.

c. Modification of an ESEP Position. Any proposal to change the scope of an ESEP participant's certification will be according to the procedures outlined in paragraph N-4a, with emphasis on the specific modification. Any proposal to extend the ESEP participant's duration must be initiated and requested by the supervisor of the host command or agency through HQ, AMC, for concurrence by the foreign executive agent, and then formally requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

N-5. Administering ESEP participants

a. Visits. All visits or travel by the ESEP participant will be according to the work being performed under the approved position description. All travel orders will identify the individual as an ESEP participant assigned to the U.S. Army host activity.

b. Library and publications support. At the discretion of the host command or activity contact officer and through coordination with the FDO, an ESEP participant may have supervised access to the CMI section of the command or agency library. Additionally, each ESEP participant may be provided a reference set of DA and or host activity publications necessary to the successful performance of the ESEP position description, consistent with the ESEP participant's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned when the ESEP participant's assignment ends.

c. Computer access. ESEP participants may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is needed to accomplish the work under his/her approved position description and is authorized for disclosure to their government. See paragraph N-2l for information on e-mail addresses and messages. In all cases, the provisions of AR 380-19 and local security procedures will apply.

d. Misconduct. ESEP participants work at the pleasure of DA and must conform to the Army's customs and traditions and comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If an ESEP participant violates the terms of certification, violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the contact officer will notify the local international POC and provide a written report on the inappropriate action through command channels to HQ, AMC.

HQ, AMC, will provide ODUSA(IA) and ODCSINT, HQDA, with a copy of the report. The report will cite full particulars and contain a recommendation for final disposition by HQ, AMC, such as temporary suspension or permanent revocation of privileges, or revocation of certification. ODUSA(IA), HQDA will coordinate the resolution of all ESEP misconduct cases.

N-6. Supervisor Functions.

The ESEP participant's supervisor will—

- a.* Ensure that the ESEP participant understands the work to be performed under the approved position description.
- b.* Ensure that the person is provided access only to that information necessary to fulfill the duties of the position description as described in the DDL, or equivalent disclosure guidance.
- c.* Inform co-workers of the access limitations related to the ESEP participant and their responsibilities in dealing with the ESEP participant.
- d.* Ensure that the ESEP participant signs a certification similar to the sample in figure N-2 before being assigned to the position.
- e.* Be familiar with this regulation, other applicable regulatory guidance governing the disclosure of CUI, and specific disclosure guidelines established in the DDL or equivalent disclosure guidance.

N-7. U.S. Contact officer.

a. Contact officers will be designated in writing by commanders or agency heads, or their designees to facilitate and oversee the activities of ESEPs at DA commands or agencies. The contact officer should be of equivalent rank/grade or higher, if available, to the ESEP. A primary and an alternate contact officer must be identified in the DDL (paragraph 8). They must be physically accessible to and have daily contact with the ESEP. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his duties. Contact officers will also adhere to the guidelines listed below. Note: In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the U.S. Army.

b. The contact officer for a ESEP will—

(1) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by ODCSINT, HQDA for the individual ESEP position.

(2) Initially brief a new ESEP on DA and local policies and procedures affecting the ESEP's status and performance of functions, as well as customs of the U.S. Army; subsequently, the contact officer will render advice and assistance to the ESEP in complying with such policies and procedures. The contact officer will have the ESEP sign a statement, similar to the document exhibited at fig N-2, indicating his or her agreement and understanding. The contact officer will provide a copy of the signed certification form to the ESEP.

(3) In conjunction with the FDO, evaluate the ESEP's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the ESEP's approved terms of certification. Consultations and visits beyond a ESEP's terms of certification require the submission of formal visit requests by the ESEP's embassy in Washington, DC.

(4) Receive, evaluate, and recommend/refer all ESEP requests for CMI to the FDO.

(5) Receive, evaluate, and refer all ESEP requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent, who will render a disclosure decision and return the action to the FDO for case closure.

(6) Notify the ODCSINT, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of ESEPs under their oversight.

(7) Notify the supporting counterintelligence and local security offices of any foreign visitor activity which is reportable under the provisions of AR 381-12.

(8) Comply with the procedures cited in paragraph N-5d of this appendix regarding misconduct on the part of the ESEP.

(9) Brief U.S. personnel with whom the ESEP will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions. The contact officer will have the ESEP participant sign a copy of the statement exhibited at figure N-2, indicating his or her agreement and understanding.

COMMITMENT ON INVENTIONS TO HOST PARTY

COMMITMENT TO HOST PARTY

In consideration for being selected to participate in the U.S.-(insert country name) Army Scientists and Engineers Exchange Program, I hereby grant to the Host Party a worldwide, non-transferable, irrevocable, non-exclusive, royalty-free license to practice (make, use, or sell) inventions (whether patentable or not patentable) and unlimited use and reproduction rights in technical information, which inventions are made (either conceived or reduced to practice) by me or which technical information is developed by me during the period of and as a result of my participation in this Program.

Additionally, to secure the rights granted above, I hereby grant to the Host Party the right to prosecute or to have prosecuted patent applications on the above mentioned inventions in any country for which the Parent Party or I choose not to prosecute a patent application.

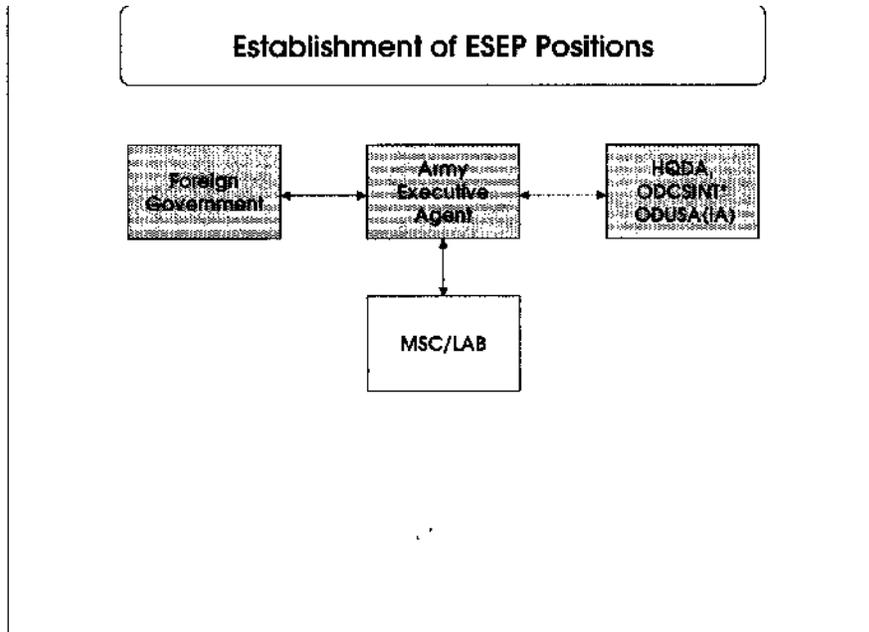
(SIGNATURE OF FOREIGN EXCHANGE OFFICER)

Figure N-1. Sample commitment to hosp party statement-ESEP

I understand and acknowledge that I have been accepted for assignment to (insert name and location of organization to which assigned) pursuant to an agreement between the (insert applicable military service or organization) of the United States and the (insert applicable foreign military organization) of (insert country name). In connection with this assignment, I further understand, acknowledge, and certify that I will comply with the following conditions and responsibilities:

1. The purpose of the assignment is to gain knowledge of the organization and management of Host Party (cite applicable area for foreign exchange personnel assignment) defense activities. There will be no access to information except as required to perform the duties described in the position description of the position to which I am assigned, as determined by my designated supervisor.
2. I will perform only functions which are properly assigned to me as described in the position description (PD) for my assignment and will not act in any other capacity on behalf of my government or my Parent Party or Parent Organization.
3. All information to which I may have access during this assignment will be treated as information provided to my government in confidence and will not be further released or disclosed by me to any other person, firm, organization or government without the prior written authorization of the Host Party.
4. When dealing with individuals outside of my immediate office of assignment on official matters, I will inform such individuals that I am a foreign exchange person.
5. I have been briefed on, understand, and will comply with all applicable security regulations of the Host Party and the Host Organization.
6. I will immediately report to my designated supervisor all attempts by unauthorized persons to obtain classified, proprietary or controlled unclassified information to which I may have access as a result of this assignment.

Figure N-2. Sample certification for ESEP person

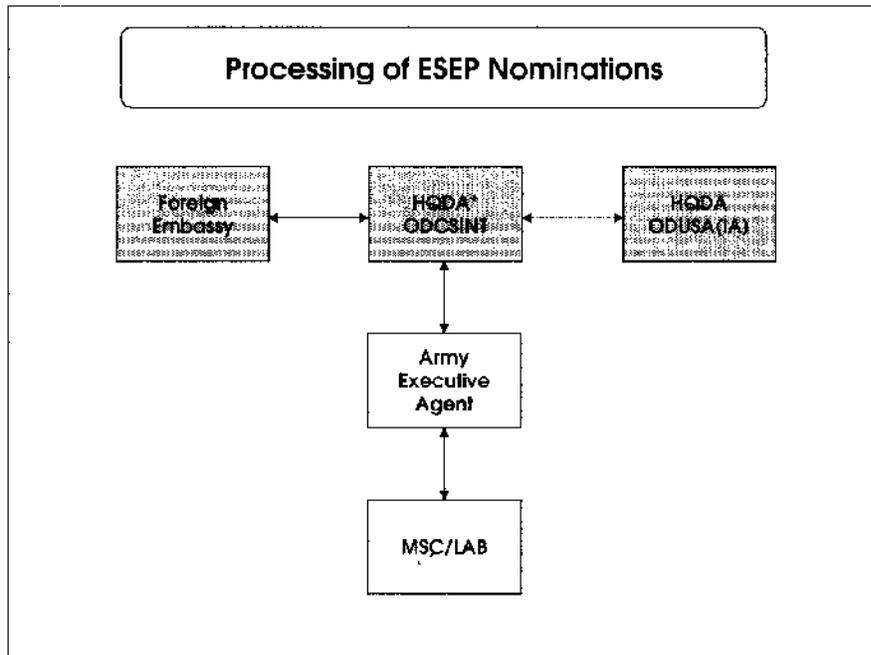


NOTES

* Shall coordinate with ODUSA(IA), as required, but shall also provide copy of EVA for information purposes.

↔ Action Tasker
 ⇄ Coordination (as required)

Figure N-3. Establishment of ESEP positions



NOTES

* Shall coordinate with ODUSA(IA), as required, but shall provide copy of EVA for information purposes.

↔ Action Tasker

↔-- Coordination (as required)

Figure N-4. Processing of ESEP nominations

Appendix O

Cooperative Program Personnel

O-1. Concept

a. Foreign nationals may be assigned to international program offices that are hosted by a DA Component as part of an international management team responsible for the implementation of a international project or program. Foreign nationals assigned to CPP positions will be military members or civilian employees of the counterpart foreign government defense organization. ODUSA(IA) is the DA proponent for this program.

b. Only foreign government personnel assigned to an international program office, hosted by an Army command or agency pursuant to the terms of a Cooperative Program International Agreement, and who report to and take direction from an Army-appointed U.S. PM (or PM-equivalent) will be accorded the treatment described in this appendix.

O-2. Conditions and Limitations.

a. CPP participants will not act in the dual capacity as foreign exchange personnel participant and as a representative of their government (for example, a FLO) while assigned to a DA command.

b. CPP participants will not serve as conduits between DA and their government for requests and transmission of CMI and CUI nor be used as a mechanism for exchanging technical data or other controlled information between the governments.

c. CPP participants will not be assigned to command or other positions that would require them to exercise responsibilities reserved by law or regulation to an officer or employee of the USG. They will not, for example, perform responsibilities of a contracting officer's technical representative, duty officer, classified document custodian or security officer, escort for foreign visitors, or perform other official acts as a representative of DA.

d. CPP participants will not be assigned to DOD contractor facilities.

e. DA will not submit ENDP requests solely to establish a CPP position.

f. The assignment of CPP participants will not be used for training foreign personnel in violation of DOD 5105.38M or, instead of, or in combination with CPP certification. Pursuant to Section 1082 of Public Law 104-201, training may not be conducted under the CPP except as necessary to familiarize, orient, or certify CPP participants regarding unique aspects of the positions to which they are assigned.

g. CPP participants will not be used for the purpose of augmenting DA staff positions or as a means to obtain personnel resources beyond authorized manning levels.

h. CPP participants will not be placed in duty positions that could result in their access to CMI or CUI that has not been authorized for disclosure to their government.

i. CPP participants will not have permanent custody of CMI and CUI. They may have access to the information during normal duty hours at the place of assignment when access is necessary to perform their duties and the information is authorized for disclosure pursuant to the DDL or equivalent disclosure guidance. In all cases, local security policies and procedures apply.

j. CPP participants' access to restricted areas will be according to AR 190-13 and local security policies and procedures and as specified in DDLs or equivalent disclosure guidance documents.

k. CPP military participants will wear their uniforms while CPP civilian participants will wear civilian attire according to local command customs and tradition. They will wear, in clear view, a DA building or installation pass or badge (if required) that clearly identifies them as foreign nationals.

l. Any other identification (including organizational code and title, block, office nameplate, security badge, or e-mail address) used by or issued to CPP participants by the host Army units will clearly identify the CPP participant's status as a foreign national. For example, an e-mail address will resemble the following: "SmithJ(Full country name National)@hqda.army.mil". Acronyms for country names will not be used. The recipient of the CPP's e-mail message must be able to identify the CPP as a foreign national.

m. CPP participants will sign, as required, a statement regarding invention rights (see fig O-1).

O-3. CPP MOA and Certification

a. MOA. AR 550-51 will govern the development of a MOA for the establishment of CPP positions. The Cooperative Program International Agreement, or an annex or implementing arrangement thereto, will cover the following issues (at a minimum):

- (1) Type of positions to be established
- (2) Length of tour

- (3) Financial responsibilities (for example, travel, salary, etc.) and use of government facilities and equipment
- (4) Entitlements (for example, commissary privileges, medical care, etc.)
- (5) Status of assigned personnel, to include privileges and exemptions, liabilities and claims
- (6) Security
- (7) Disciplinary matters
- (8) Administrative matters and oversight responsibilities (for example, leave, dress, reviews, and performance reports)

(9) Identification

b. Certification.

(1) CPP participants are certified to DA commands or agencies to perform assigned duties. Terms of certification are derived from and are consistent with the scope of the MOA.

(2) Each CPP participant must sign a certification statement acknowledging the terms of his or her assignment (see fig O-2). A copy of the signed certification statement, which will be maintained by the local FDO, must be provided to the CPP. If the CPP participant refuses to sign the certification statement, the command or agency must immediately notify ODCSINT, HQDA, which will notify the DA proponent and together resolve the issue through the parent government's military attaché in Washington, D.C.

O-4. Establishment of CPP Positions and Processing of CPP Nominations.

a. Establishment of CPP Positions. DA commands and agencies desiring to have CPPs certified and assigned to them must formally obtain HQDA concurrence. A request for a new CPP position will not be finalized unless the respective foreign government has signed an international MOA. The procedures for establishing a new CPP position (fig K-3) are as follows:

(1) Request Initiated by a Foreign Government for Establishment of a CPP Position.

(a) Step 1: If a foreign government initiates a request for the establishment of a CPP position with the U.S. Army, ODUSA(IA), HQDA will notify the affected command or agency in writing and request a recommendation on the establishment of the proposed CPP position. Such proposals will be conveyed in writing through command or agency channels. For example, if the request involves the assignment of a CPP to a PEO PM office, ODUSA(IA), HQDA will send the proposal to OASA(ALT) for staffing to the appropriate PEO PM.

(b) Step 2: The specified DA command or agency will evaluate the proposal and submit to ODUSA(IA), HQDA a recommendation to approve or disapprove the proposal. If the proposal involves the assignment of a CPP to the office of a PEO PM, the PM will coordinate his or her position with the MSC matrix support and submit the coordinated position to OASA(ALT), which will forward the response to ODUSA(IA), HQDA. CPP position proposals must provide—

- 1. Title of the position.
- 2. Position location.
- 3. Qualification and skills required.
- 4. Description of specific duties of the position.
- 5. Classified access level required.

6. Draft DDL or equivalent document containing data elements of a DDL. Note: According to DODD 5230.20, an equivalent document containing data elements of a DDL is required for positions necessitating access to only unclassified information. The local commander may approve this document with a copy furnished to ODCSINT, HQDA.

7. Clearly demonstrate or anticipate a mutual need for the position. The rationale must clearly demonstrate the requirement for the CPP's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve best interests of the U.S. Army.

(c) Step 3: ODUSA(IA), HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: ODCSINT, OASA (ALT), ODCSOPS, OTJAG, and the subject matter expert, if different from the preceding offices.

(d) Step 4: After HQDA coordination is completed, ODUSA(IA), HQDA will finalize the decision on the proposal and formally notify the appropriate foreign government embassy. If the proposal is approved, the DA command or agency to which the CPP will be assigned will immediately begin to finalize the position DDL for approval and issuance by ODCSINT, HQDA. Upon receipt of the final draft DDL proposal from ODUSA(IA), HQDA, ODCSINT, HQDA will staff the final draft DDL with the HQDA offices cited in Step 3 (above) and other appropriate agencies. Upon concurrence and approval of the DDL, ODUSA(IA), HQDA, will notify the hosting Army command or agency and the appropriate foreign military attaché. The approved DDL will be in place prior to the submission of the EVA request by the appropriate foreign military attaché.

(2) Request Initiated by a DA Command or Agency for Establishment of a CPP Position.

(a) Step 1: Prior to beginning discussions with foreign representatives on the establishment of a CPP position, DA

commands or agencies must obtain ODUSA(IA), HQDA permission to proceed. Such proposals will be conveyed in writing through command or agency channels to ODUSA(IA), HQDA. Proposals conveyed through PEO PMs will be sent to OASA(ALT) for forwarding to ODUSA(IA), HQDA.

(b) *Step 2:* A DA command or agency will provide the following information in support of its initiative to establish a CPP position:

1. Title of the position.
2. Position location.
3. Qualification and skills required.
4. Description of specific duties of the position.
5. Classified access level required.
6. Draft DDL or equivalent document containing data elements of a DDL. Note: according to DODD 5230.20, an equivalent document containing data elements of a DDL is required for positions necessitating access to only unclassified information. The local commander may approve this document with a copy furnished to ODCSINT, HQDA.

7. Clear statement of need for the position. The rationale must clearly demonstrate the requirement for the CPP's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve best interests of the U.S. Army.

(c) *Step 3:* ODUSA(IA), HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: ODCSINT, OASA (ALT), ODCSOPS, OTJAG, and the subject matter expert, if different from the preceding offices.

(d) *Step 4:* After HQDA coordination is completed, ODUSA(IA) will finalize the decision on the initiative and formally submit the proposal to the appropriate foreign government embassy. If the latter is receptive to the proposal, ODUSA(IA) will direct the negotiations for DA. While the negotiations are being conducted, the DA command or agency that initiated the proposal will immediately begin to finalize the draft position DDL for approval and issuance by ODCSINT, HQDA. Upon receipt of the final draft DDL from ODUSA(IA), HQDA, ODCSINT, HQDA will staff the document with the HQDA offices cited in Step 3 (above) and other appropriate agencies. Upon concurrence and approval of the DDL, ODCSINT, HQDA will hold the document, awaiting conclusion of the negotiations and formal agreement to establish a CPP position. Upon establishment of the CPP position, the approved DDL will already be in place awaiting the submission of the EVA request by the appropriate foreign military attaché.

b. *Processing of CPP Nominations.* If the CPP position is established, ODCSINT, HQDA will process the assignment of the CPP to a DA command or agency (see fig K-4) in the following manner:

(1) *Step 1:* The appropriate foreign military attaché will submit an EVA request at least 45 days prior to the requested date of arrival/assignment of the CPP. In the EVA request, the foreign military attaché provides written notification to ODCSINT, HQDA of the following—

- (a) Subject individual is an officially-sponsored official of that government.
- (b) Such official is authorized by the sponsoring government to perform duties under a MOA.
- (c) The official holds a specified level of security clearance.
- (d) The parent government will assume the responsibility for any and all U.S. CMI provided to the CPP.

(2) *Step 2:* ODCSINT, HQDA will process the EVA request to the DA command or agency (PEO PM through its matrix support) to which the CPP is to be assigned. Since the DDL outlining the terms of the certification of the CPP was pre-coordinated and approved, the recipient DA command or agency should respond favorably within 20 working days of the receipt of the EVA request. The DDL will remain valid until there is a change to the scope of the duties or the position is terminated. See appendix E for detailed information on DDLs.

(3) *Step 3:* Upon receipt of the concurrence of the recipient DA command or agency, ODCSINT, HQDA will approve the EVA request and notify the recipient DA command or agency of the approval. The foreign military attaché will then coordinate with the recipient DA command or agency for the arrival of the CPP. Note: DA commands or agencies may not accept a CPP until the DDL and visit request have been approved. If a CPP arrives prior to visit approval, the DA command or agency involved will not permit the CPP to commence his or her duties. The DA command or agency FDO must be notified immediately. The DA command or agency FDO will then notify the ODCSINT, HQDA, who will coordinate the disposition of CPP with ODUSA(IA) and the appropriate foreign military attaché, and provide instructions to the DA command or agency FDO.

c. *Modification of a CPP Position.* Any proposal to change the scope of a CPP's certification will be according to the procedures outlined in paragraphs O-4a(1) and O-4a(2), with emphasis on the specific modification. Any proposal to extend the CPP's duration must be initiated and requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

d. *Reevaluation of a CCP Position.* Once established, each CPP position and the associated DDL will be reevaluated on each successive nomination to ensure that the best interests of the host command or agency and DA continue to be served, and the purpose of the position remains valid. To alleviate the possibility of a CPP arriving to assume an established position prior to visit approval, ODCSINT, HQDA will initiate contact with the appropriate foreign

government Military Attaché in Washington, DC 90 days prior to the tour expiration date of the incumbent CPP and query the foreign military attaché concerning a replacement for the position, extension of the incumbent CPP, or other alternatives contemplated by the parent government. The ODCSINT, HQDA will also inform the sponsoring Army command or agency of the intended action, if any, of the foreign government to alter the status of the CPP position. The host command or agency FDO and contact officer will also commence their reevaluation 90 days prior to the tour expiration date of the incumbent CPP.

O-5. Administering CPP Participants.

a. Visits. All visits or travel by the CPP participant will be according to the standing operating procedures of the command or agency of assignment. However, all travel orders will identify the individual as a CPP participant assigned to the U.S. Army. ODUSA(IA) approval is required for all OCONUS travel by any CPP participant.

b. Library and publications support. At the discretion of the host activity, a CPP may be granted supervised access to the CMI section of a command or agency library. Additionally, each CPP may be provided a reference set of DA and activity publications necessary to the successful performance of the CPP's duties, consistent with the CPP's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the CPP's successor when the CPP's certification ends.

c. Computer access. CPPs may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is authorized for disclosure to their government. See paragraph O-21 for information regarding e-mail addresses and messages. In all cases, the provisions of AR 380-19 and local security procedures will apply.

d. Misconduct. CPPs serve at the pleasure of DA and must conform to the Army's customs and traditions and comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If a CPP violates the terms of certification; violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the contact officer will notify the local agency or command FDO and provide a written report on the inappropriate action through command channels to ODUSA(IA), with a copy furnished to ODCSINT, HQDA. The report will cite full particulars and contain a recommendation for final disposition by HQDA, such as temporary suspension or permanent revocation of privileges, or revocation of certification. ODUSA(IA) will coordinate the resolution of all misconduct cases.

e. Supervisor functions. DA officials designated to supervise a CPP participant —

- (1) Ensure that the CPP participant understand the duties to be performed in the assigned position.
- (2) Ensure that the CPP participant is provided access only to that CMI and CUI necessary to fulfill the duties of the position description as described in the DDL or equivalent disclosure guidance.
- (3) Be familiar with this regulation, other applicable regulatory guidance governing the disclosure of CUI, and specific disclosure guidelines established in the DDL or equivalent disclosure guidance.
- (4) Inform co-workers of the disclosure limitations on access to CMI and CUI related to the CPP participant and their responsibilities in dealing with the CPP participant.
- (5) Ensure that the CPP participant signs a certification similar to the sample in figure O-2 before being assigned to the position.

f. U.S. contact officer.

(1) Contact officers will be designated in writing by commanders or agency heads, or their designees to facilitate and oversee the activities of CPPs at DA commands or agencies. The contact officer should be of equivalent rank/grade or higher, if available, to the CPP. A primary and an alternate contact officer must be identified in the DDL (para 8). They must be physically accessible to and have daily contact with the CPP. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his duties. Contact officers will also adhere to the guidelines listed below. Note: In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the U.S. Army.

(2) The contact officer for a CPP will—

(a) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by ODCSINT, HQDA for the individual CPP position.

(b) Initially brief a new CPP on DA and local policies and procedures affecting the CPP's status and performance of functions, as well as customs of the U.S. Army; subsequently, the contact officer will render advice and assistance to the CPP in complying with such policies and procedures. The contact officer will have the CPP sign a statement, similar to the document exhibited at figure O-2, indicating his or her agreement and understanding. The contact officer will provide a copy of the signed certification form to the CPP.

(c) In conjunction with the FDO, evaluate the CPP's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the CPP's approved terms of certification. Consultations and visits beyond a CPP's terms of certification require the submission of formal visit requests by the CPP's embassy in Washington, D.C.

- (d) Receive, evaluate, and recommend/refer all CPP requests for CMI to the FDO.
- (e) Receive, evaluate, and refer all CPP requests involving CUI to the FDO for administrative processing and forwarding to the originator/proponent, who will render a disclosure decision and return the action to the FDO for case closure.
- (f) Notify the ODCSINT, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of CPPs under their oversight.
- (g) Notify the supporting counterintelligence and local security offices of any foreign visitor activity that is reportable under the provisions of AR 381-12.
- (h) Comply with the procedures cited in paragraph O-5d of this appendix regarding misconduct on the part of the CPP.
- (i) Brief U.S. personnel with whom the CPP will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions. The contact officer will have the CPP participant sign a copy of the statement exhibited at figure O-2, indicating his agreement and understanding.

COMMITMENT TO HOST PARTY

In consideration for being selected to participate in the U.S.-(insert country name) Army Cooperative Program Personnel, I hereby grant to the Host Party a worldwide, non-transferable, irrevocable, non-exclusive, royalty-free license to practice (make, use, or sell) inventions (whether patentable or not patentable) and unlimited use and reproduction rights in technical information, which inventions are made (either conceived or reduced to practice) by me or which technical information is developed by me during the period of and as a result of my participation in this Program.

Additionally, to secure the rights granted above, I hereby grant to the Host Party the right to prosecute or to have prosecuted patent applications on the above mentioned inventions in any country for which the Parent Party or I choose not to prosecute a patent application.

(SIGNATURE OF FOREIGN EXCHANGE OFFICER)

Figure O-1. Sample commitment to host party statement-CPP

I understand and acknowledge that I have been accepted for assignment to (insert name and location of Cooperative Program to which assigned) pursuant to an agreement between the (insert applicable military service or organization) of the United States and the (insert applicable foreign military organization) of (insert country name). In connection with this assignment, I further understand, acknowledge, and certify that I will comply with the following conditions and responsibilities:

1. The purpose of the assignment is to provide my expertise to the Cooperative Program. There will be no access to information except as required to perform the duties described in the position description (PD) of the position to which I am assigned, as determined by my designated supervisor.

2. I will perform only functions which are properly assigned to me as described in the PD for my assignment and will not act in any other capacity on behalf of my government or my Parent Party or Parent Organization.

3. All information to which I may have access during this assignment will be treated as information provided to my government in confidence and will not be further released or disclosed by me to any other person, firm, organization or government without the prior written authorization of the Cooperative Program.

Figure O-2. Sample certification for CPP participant

4. When dealing with individuals outside of my immediate office of assignment on official matters, I will inform such individuals that I am a foreign Cooperative Program person.

5. I have been briefed on, understand, and will comply with all applicable security regulations of the Cooperative Program.

6. I will immediately report to my designated supervisor all attempts by unauthorized persons to obtain classified, proprietary or controlled unclassified information to which I may have access as a result of this assignment.

Figure O-2. Sample certification for CPP participant—Continued

Glossary

Section I Abbreviations

ABCA

American, British, Canadian and Australian Armies Standardization Program

ACTD

Advanced Cooperative Technology Demonstration

AECA

Arms Export Control Act

AMC

U.S. Army Materiel Command

AR

Army regulation

ARMA

U.S. Army Military Attaché

ASA(ALT)

Assistant Secretary of the Army (Acquisition, Logistics, and Acquisition)

ATPO

Associate Technical Project Officer

BMDO

Ballistic Missile Defense Organization

CBD

Commerce Business Daily

CG

Commanding General

CIA

Central Intelligence Agency

CJCS

Chairman, Joint Chiefs of Staff

CMI

classified military information

COE

Chief of Engineers

COMSEC

communications security

CONUS

continental United States

CPI

Critical Program, Information, Technology, and System

CPP

cooperative program personnel

CSA

Chief of Staff, Army

CUI

controlled unclassified information

DA

Department of the Army

DAS

Director of the Army Staff

DCI

Director of Central Intelligence

DCS

direct commercial sales

DCSINT

Deputy Chief of Staff for Intelligence

DCSLOG

Deputy Chief of Staff for Logistics

DCSOPS

Deputy Chief of Staff for Operations and Plans

DCSPER

Deputy Chief of Staff for Personnel

DDEP

Defense Development Exchange Program

DDL

Delegation of Disclosure Authority Letter

DEA

Data Exchange Agreement

DIA

Defense Intelligence Agency

DISC4

Director of Information Systems for Command, Control, Communications and Computers

DOD

Department of Defense

DODD

Department of Defense directive

DODI

Department of Defense instruction

DSS

Defense Security Service

DTIC

Defense Technical Information Center

DUSA(IA)

Deputy Under Secretary of the Army (International Affairs)

DUSA(OR)

Deputy Under Secretary of the Army (Operations Research)

EAA

Export Administration Act

EAR

Export Administration Regulations

ECP

engineering change proposal

ENDP

exception to national disclosure policy

EPITS

Essential Program Information, Technology, and System

ESEP

Engineers and Scientists Exchange Program

EVA

extended visit authorization

FDO

foreign disclosure officer

FIS

foreign intelligence service

FLO

foreign liaison officer

FMS

foreign military sales

FOCI

foreign ownership, control or influence

FORDTIS

Foreign Disclosure and Technical Information System

FORSCOM

U.S. Army Forces Command

FVS

Foreign Visits System

GPO

Government Printing Office

GSOMIA

General Security of Military Information Agreement

HQ

headquarters

HQDA

Headquarters, Department of the Army

IATS

International Agreements Tracking System

IEA

information exchange annex

IMET

International Military Education and Training

INSCOM

US Army Intelligence and Security Command

ITAR

International Traffic in Arms Regulations

ITO

invitational travel orders

JCO

Joint Certification Office

JCP

Joint Certification Program

JCS

Joint Chiefs of Staff

LATAM

Latin America

LOA

Letter of Offer and Acceptance

MACOM

major Army Command

MCTL

Militarily Critical Technologies List

MOA

Memorandum of Agreement

MOP

Memorandum of Policy

MOU

Memorandum of Understanding

MPEP

Military Personnel Exchange Program

MSC

major subordinate command

MWO

modification work order

MWDDEP

Mutual Weapons Development Data Exchange Program

NATO

North Atlantic Treaty Organization

NDP or NDP-1

National Disclosure Policy

NDPC

National Disclosure Policy Committee

NIAG

NATO Industrial Advisory Group

NIPRNET

Non-Secure Internet Protocol Router Network

NISPOM

National Industrial Security Program Operating Manual

NMS

National Military Strategy

NORAD

North American Defense

NSO

National Standardization Officer

NSS

National Security Strategy

NTIS

National Technical Information Service

OCONUS

outside the continental United States

ODCSINT

Office of the Deputy Chief of Staff for Intelligence

ODCSOPS

Office of the Deputy Chief of Staff for Operations and Plans

ODUSA(IA)

Office of the Deputy Under Secretary of the Army for International Affairs

OJCS

Office of the Joint Chiefs of Staff

OPSEC

operations security

OSD

Office of the Secretary of Defense

OT

orientation tours

OUSD(P)

Office of the Under Secretary of Defense (Policy)

P&A

price and availability

PCO

procuring contracting officer

PEO

program executive office

PEP

Personnel Exchange Program

PIP

product improvement proposal

PM

program or project manager

POC

point of contact

PPP

Program Protection Plan

QAP

Quadripartite Advisory Publication

QSTAG

Quadripartite Standardization Agreement

QWG

Quadripartite Working Group

RA

record of action

RAC

request for authority to conclude

RAN

request for authority to negotiate

R&D

research and development

RDT&E

research, development, test and evaluation

RFI

request for information

RFP

request for proposal

RSI

rationalization, standardization, and interoperability

RVA

request for visit authorization

SAO

Security Assistance Office

SCI

sensitive compartmented information

SEEP

Scientists and Engineers Exchange Program

SIPRNET

Secret Internet Protocol Router Network

SMDC

Space and Missile Defense Command

SSA

Special Security Agreement

SSOI

Summary Statement of Intent

StanRep

Standardization Representative

TA/CP

Technology Assessment/Control Plan

TAGO

The Adjutant General's Office

TCP

Technology Control Panel

TJAG

The Judge Advocate General

TPO

technical project officer

TRADOC

U.S. Army Training and Doctrine Command

TRDP

technology research and development program

TSG

The Surgeon General

TTCP

The Technical Cooperation Program

U.S.

United States

USACIDC

U.S. Army Criminal Investigation Command

USASAC

U.S. Army Security Assistance Command

USC

United States Code

USDAO

United States Defense Attaché Office

USG

United States Government

VCSA

Vice Chief of Staff, Army

Section II**Terms****ABCA Primary Standardization Office**

ABCA Primary Standardization Office (PSO) acts as the official office or record for the ABCA program. Provides continuous review of program and recommends action to expedite progress or resolve differences. The ABCA PSO is located within the ODUSA(IA).

Acquisition-related meeting

Meeting at which information to be presented describes DA activities related to known or anticipated procurement of materiel to satisfy actual or projected requirements. Such meetings include, but are not limited to, Advanced Planning Briefings for Industry and pre-solicitation proposal, pre-bidder, and pre-award meetings.

Agency

A separate table of distribution and allowances organization under the direct supervision of HQDA. An agency can be functionally described as having either a staff support of field operating mission. A unit or organization which has primary responsibility for performing duties or functions as representative of, and with the assigned authority of, the headquarters to which it is subordinate. A PM under the PEO system is an agency.

Associate Technical Project Officer (ATPO)

The individual responsible for assisting in the overall technical management of the DEA, including exchange of data and information.

Attaché

A diplomatic official or military officer attached to an embassy or legation, especially in a technical capacity.

Budget activities – RDT&E

a. Budget Activity 1 (BA1) - BASIC RESEARCH. Basic research efforts provide fundamental knowledge for the solution of identified military problems. Includes all efforts of scientific study and experimentation directed toward increasing knowledge and understanding in those fields of physical, engineering, environmental, and life sciences related to long-term national security needs. It provides farsighted, high payoff research, including critical enabling technologies that provide the basis for technological progress. It forms a part of the base for—

- (1) subsequent exploratory and advanced developments in defense-related technologies, and
- (2) new and improved military functional capabilities in areas such as communications, detection, tracking, surveillance, propulsion, mobility, guidance and control, navigation, energy conversion, materials and structures, and personnel support. Basic research efforts precede the system-specific research described in DODD 5000.1.

b. Budget Activity 2 (BA2) - EXPLORATORY DEVELOPMENT. This activity translates promising basic research into solutions for broadly defined military needs, short of major development projects, with a view to developing and evaluating technical feasibility. This type of effort may vary from fairly fundamental applied research to sophisticated breadboard hardware, study, programming and planning efforts that establish the initial feasibility, and practicality of proposed solutions to technological challenges. It would thus include studies, investigations, and non-system specific development efforts. This dominant characteristic of this category of effort is that it be pointed toward specific military needs with a view toward developing and evaluating the feasibility and practicability of proposed solutions and determining their parameters. Program control of the Exploratory Development will normally be exercised by a general level of effort. Exploratory Development precedes the system-specific research described in DODD 5000.1.

c. Budget Activity 3 (BA3) - ADVANCED DEVELOPMENT. Includes all efforts which have moved into the

development and integration of hardware and other technology products for field experiments and test. The results of this type of effort are proof of technological feasibility and assessment of operability and producibility that could lead to the development of hardware for service use. It also includes advanced technology demonstrations that help expedite technology transition from the laboratory to operational use. Projects in this category have a direct relevance to identified military needs. Advanced Development may include concept exploration as described in DODD 5000.1, but is system specific.

Certification

Formal recognition by DA of a working relationship with a representative of a foreign government (for example, a FLO) for specified purposes and on an extended basis over an agreed period of time.

Classified contract

Any contractual agreement that requires, or will require, access to classified information (Confidential, Secret, or Top Secret) by the contractor or its employees in the performance of the contract. The contract may be a classified contract even though contract document is not classified.

Classified military information (CMI)

Information originated by or for the Department of Defense or its Agencies or under their jurisdiction or control, which requires protection in the interest of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL as described in E.O. 12958 or subsequent order. Classified military information may be in oral, visual, documentary, or materiel form. DOD Directive 5230.11 and AR 380-10 provide details of the eight categories into which classified military information has been subdivided.

Combined information

Military information that, by agreement, is declared to be combined by the U.S. Government and one or more other national governments (or an international organization), irrespective of origin of information.

Contact officer

A DA official designated in writing to oversee and facilitate all contacts, requests for information, consultations, access, and other activities of foreign nationals who are assigned to, or are visiting, a DA component or subordinate organization. The identification of the contact officer in an approved RVA is recognized as designation in writing. In the cases of foreign exchange and cooperative personnel, the host supervisor may be the contact officer.

Controlled unclassified information (CUI)

Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the U.S. Government (USG). It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.24, DODD 5230.25, DODD 5400.7, AR 25-55, AR 70-31, AR 340-21, AR 530-1, etc., or that is subject to export controls according to the ITAR or the EAR. For the purposes of this regulation, this definition of CUI will apply.

Cooperative Program

A program for research, development, test, evaluation, and/or production that is not implemented under the Security Assistance Program.

Cooperative Program Personnel

Foreign government personnel, assigned to a multinational program office that is hosted by DA pursuant to the terms of a Cooperative Program International Agreement, who report to and take direction from a DA-appointed Program Manager (or Program Manager equivalent) for the purpose of carrying out the multinational project or program. Foreign government representatives described in such agreements as liaison officers or observers are not considered Cooperative Program Personnel and will be treated as FLOs.

Co-production

Method by which items intended for military application are produced or assembled under provisions of a formal agreement that provides for transfer of technical information and know-how from one government to another.

Critical technology

Technology that consists of—

- a. Arrays of design and manufacturing know-how (including technical data).
- b. Keystone manufacturing, inspection, and test equipment.
- c. Keystone materials.
- d. Goods accompanied by sophisticated operation, application, or maintenance know-how that would make a

significant contribution to military potential of any country—or combination of countries—and compromise of which may prove detrimental to U.S. security.

Data Exchange Annex (DEA)

An annex of the master data/information exchange agreement that identifies the specific area in which R&D information will be exchanged and the organizations authorized to implement the DEA.

Defense information/technology

Any weapons, weapon system, munitions, aircraft, vessel, boat, or other implement of war; any property, installation, commodity, materiel, equipment, supply, or goods used for the purposes of furnishing military assistance or making military sales; any tool, machinery, facilities, materiel, supply, or other item necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any other defense articles; or any component or part of the preceding articles—less merchant vessels and articles governed by the Atomic Energy Act of 1954, as amended

Defense Service

Any service, test, inspection, repair, training, publication, or technical or other assistance, or defense information used for the purpose of furnishing security assistance-less design and construction services.

Delegation of Disclosure Authority Letter (DDL)

A letter issued by the appropriate Designated Disclosure Authority describing classification levels, categories, scope, and limitations related to information under DA's disclosure jurisdiction that may be disclosed to specific foreign governments or their nationals for a specified purpose.

Designated Disclosure Authority

An official, designated by the Head of DA or by DA's Principal Disclosure Authority, who has been delegated disclosure authority according to DOD Directive 5230.11, to control disclosures by subordinate commands or staff elements of classified military information to foreign governments and their nationals and to international organizations.

Disclosure

Conveying of CMI to an authorized representative of a foreign government. Disclosures may be accomplished through oral, visual, or documentary modes.

Document/documentary materiel

Any recorded information, regardless of its medium, physical form, or characteristics.

Engineers and Scientists Exchange Program (ESEP)

A program under which civilian and military scientists and engineers, pursuant to the terms of an international agreement, are assigned to DA research, development, test, and evaluation facilities to conduct research, development, test and evaluation work. ESEP is the DOD acronym for the program. The U.S. Army name for the program is Scientists and Engineers Exchange Program (SEEP).

Executive agent

The DA office or organization that has overall responsibility and oversight for a foreign exchange agreement.

Extended visit authorization

See Visit authorization.

Facility clearance

Often referred to as Limited Clearance Facility. An administrative determination that the facility is eligible, from a security viewpoint, for access to classified information of the same or lower security category as the level of clearance being granted. Facility clearances will not be granted to contractor activities located outside the United States, Puerto Rico, or a U.S. possession or trust territory.

Foreign Counterpart Visit Program (FCVP)

A program managed by Director, DIA, for coordinating all hosted visits by foreign government counterparts to the Secretary of Defense, Deputy Secretary of Defense, Chairman of the Joint Chiefs of Staff, and Vice Chairman of the Joint Chiefs of Staff.

Foreign Disclosure Officer (FDO)

DA member designated in writing to oversee and control coordination of specific disclosures of CMI and CUI. FDOs are authorized for appointment to lowest command level that is the proponent for Army-created, developed, or derived CMI and CUI.

Foreign Disclosure and Technical Information System (FORDTIS)

Automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release CMI and to deny CUI to foreign governments.

Foreign exchange personnel

Military or civilian officials of a foreign defense establishment who are assigned to a U.S. DOD Component (such as the U.S. Army), according to the terms of an applicable Exchange Agreement, and who perform duties, prescribed by a position description, for the DOD Component.

Foreign interest

Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its possessions and trust territories; and any person who is not a citizen or national of the United States.

Foreign liaison officer (FLO)

A foreign government military member or civilian employee, who is authorized his or her government, to act as an official representative of that government in its dealings with the U.S. Army in connection with programs, projects or agreements of mutual interest to the U.S. Army and the foreign government. There are three types of FLOs—

a. Security Assistance. A foreign government representative who is assigned to a DA element or contractor facility pursuant to a requirement that is described in a Foreign Military Sales Letter of Offer and Acceptance.

b. Operational. A foreign government representative who is assigned to DA element pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education. A StanRep is an operational FLO.

c. National Representative. A foreign government representative who is assigned to his or her national embassy or legation in Washington, D.C. (for example, an attaché), to conduct liaison activities with HQDA and DA element.

Foreign national

A person who is not a citizen or national of the U.S. or its territories. This definition does not include permanent residents (formerly immigrant aliens, resident aliens, or intending U.S. citizens). For the purposes of this regulation, a private non-U.S. citizen or national having no official affiliation with his or her government of origin. See definition of foreign representative.

Foreign ownership, control, or influence (FOCI)

Situation in which a foreign national, firm, or government is assumed to possess dominance of or authority over a U.S. firm to such a degree that the foreign entity may gain unauthorized access to U.S. CMI.

Foreign representative

For the purposes of this regulation, foreign representatives are foreign nationals or U.S. citizens or nationals who are acting as representatives of a foreign government, or firm or person sponsored by a foreign government. These individuals may interact officially with DA elements only in support of an actual or potential USG program (for example, FMS, USG contract, or international agreement).

Foreign Visits System (FVS)

The automated system, operated by the Office of the Under Secretary of Defense (Policy) (OUSD(P)), that provides staffing and data base support for processing requests for visits by foreign nationals to DOD activities and defense contractors. FVS consists of an unclassified segment that allows the on-line submission of visit requests from Embassies in Washington, D.C., and, in some cases, directly from foreign governments overseas. FVS also has a classified segment that provides staffing, decision-making support, and data base capabilities to the Military Departments and DIA.

Functional Agreement

An agreement not formally deemed to be an international agreement, including—

- a.* Contracts made under the Federal Acquisition Regulations.
- b.* FMS Credit Agreements.
- c.* FMS LOAs or Defense Sales Agreements.
- d.* FMS Letters of Intent.
- e.* Standardization Agreements or Quadripartite Standardization Agreements that record the adoption of like or similar military equipment, ammunition, supplies, or stores; or operational, logistic, or administrative procedures.
- f.* Leases under 10 USC 2667 or 2675.
- g.* Leases under 22 USC 2796.
- h.* Agreements that establish only administrative procedures.

Hosted visit

A visit by official nationals of a foreign government under the auspices of an invitation that is extended by a DA official.

Government-to-Government channels

Principle method that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed on by the governments involved. In either case, information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.

Information

Knowledge in a communicable form.

In-house meeting

A meeting attended exclusively by military personnel or civilian employees of DA (may be expanded to include DA contractor personnel, but only if the meeting is related exclusively to matters involving a specific contract already let).

International activities and projects

DA actions and initiatives formally accomplished under auspices both of various international agreements-bilateral and multilateral-and functional agreements, as defined in AR 550-51. Selected examples are MOUs promoting RSI among NATO and ABCA member nations and MOUs providing for cooperative R&D, including co-development, dual production, DDEPs, and security assistance programs.

International Agreement

- a.* An agreement, but not a functional agreement, that is concluded with one or more foreign governments (including their agencies, instrumentalities, or political subdivisions) or with an international organization and—
 - (1) Is signed or agreed to by one of the following:
 - (a)* civilian or military officers,
 - (b)* employees of any DOD organizational element, or
 - (c)* representatives of the Department of State or other agencies of the USG.
 - (2) Signifies the intention of the parties to be bound in international law.
 - (3) Is identified as one of the following: international agreement, Memorandum of Understanding, exchange of notes, exchange of letters, technical arrangement, protocol, note verbal, aide memoir, agreed minute, plan, contract, arrangement, or some other name having similar legal consequence.
- b.* Any oral agreement that meets the criteria in a above, Such an agreement must be reduced to writing by the DOD representative who enters into the agreement.
- c.* A NATO Standardization Agreement that provides for either of the following—
 - (1) mutual support or cross-servicing of military equipment, ammunition, supplies, and stores, or
 - (2) mutual rendering of defense services, including training.

International Organization

Entity established by recognized governments pursuant to international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

International Traffic in Arms Regulations (ITAR)

Department of State implementation of section 38 of the Arms Export Control Act. ITAR governs export of information and materiel that are defense-related and listed on the U.S. Munitions List.

International Visits Program (IVP)

The program that is established to process visits by and assignments of foreign nationals to the DOD Components and DOD contractor facilities. It is designed to ensure that classified and controlled unclassified information to be disclosed to them has been properly authorized for disclosure to their governments, to ensure that the requesting foreign government provides a security assurance on the individuals when classified information is involved in the visit or assignment, and to facilitate administrative arrangements (for example, date, time, and place) for the visit or assignment.

Intelligence

Information and related materiel describing U.S. foreign intelligence sources and methods, equipment, and methodology unique to the acquisition or exploitation of foreign intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U.S. foreign intelligence collection efforts. May or may not include SCI.

Joint information

Military information over which two or more DA, or two or more Federal departments or agencies, exercise control, jurisdiction, or security awareness.

Letter of Special Accreditation

Document that recognizes and accredits a foreign military attaché to conduct official direct contact with the U.S. Army. The document may include authorization for a foreign military attaché to effect direct contact with DA officials of a specified DA command or agency without prior permission of HQDA (Chief of Foreign Liaison, ODUSA(IA), ODCSINT, or the Public Affairs Office).

Meeting

Any conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified or controlled unclassified information is disclosed.

Military information

Classified or unclassified information under control and jurisdiction of DA or its elements, or of primary interest to them. (May be embodied in equipment or may be in written, oral, visual, or other communicable form.)

Military Personnel Exchange Program (MPEP)

A program under which military and civilian personnel of the Department of the Army and military and civilian personnel of the defense ministries and/or military services of foreign governments, pursuant to the terms of an international agreement, occupy positions with and perform functions for a host organization to promote greater understanding, standardization, and interoperability. MPEP is the DOD acronym for the program. The U.S. Army name for the program is Personnel Exchange Program (PEP).

Munitions license

A document bearing the word license issued by the Director, Office of Defense Trade Controls or his/her authorized designee which permits the export of a specific defense article or defense service controlled by the ITAR.

Munitions list

Listing of articles designated as arms, ammunition, and implements of war and are subject to licensing requirements imposed by Arms Export Control Act through ITAR.

National Disclosure Policy (NDP-1)

NDP-1 promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance required by U.S. departments and agencies having occasion to disclose CMI to foreign governments and international organizations. In addition, it establishes and provides for management of interagency mechanism and procedures required for effective implementation of the policy. This policy is based on NSDM 119, Disclosure of Classified United States Military Information to Foreign Governments and International Organizations, 20 July 1971, as reaffirmed and augmented by White House Memorandum of the same subject, date 6 June 1978.

National Disclosure Policy Committee (NDPC)

Central authority for formulation, promulgation, administration, and monitoring of the NDP-1. Consists of general and

special members and their alternates. General members have a broad interest in all aspects of committee operations. Special members have a significant interest in some, but not all, aspects of committee operations.

a. General Members will serve as representatives of the Secretaries of State, Defense, Army, Navy, and Air Force; and the Chairman, Joint Chiefs of Staff.

b. Special Members will serve as representatives of the Secretary of Energy; Director of Central Intelligence; Under Secretary of Defense for Policy; Under Secretary of Defense for Acquisition; Assistant Secretary of Defense for Command, Control, Communications and Intelligence; Assistant to Secretary of Defense (Atomic Energy); Director, Defense Intelligence Agency and Director, Strategic Defense Initiative Organization.

One-time visit authorization

See visit authorization

Originating classification authority

An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to originally classify information.

Originating classification

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Proponent

Army organization or staff element that has primary responsibility for materiel or subject matter expertise in its area of interest or charged with accomplishment of one or more functions.

Proprietary information

Information, for example, trade secrets, owned by a private individual or other entity.

Rationalization, Standardization, and Interoperability (RSI)

Means of increasing coalition warfare capabilities of US, allied, and friendly nation forces through use of common (standard) or interoperable procedures and resources. Applicable to concepts, doctrine, tactics, logistics, procedures, training, and materiel and non-materiel requirements, and is essential to successful integration of allied forces during conduct of combined operations.

Record of action (RA)

Official record of NDPC decisions on ENDP requests.

Recurring visit authorization

See visit authorization

Security assistance

Group of programs authorized by Foreign Assistance Act of 1961, as amended, and Arms Export Control Act, as amended, and Arms Export Control Act, as amended, or other related statutes by which the USG provides defense articles, military training, and other defense-related services to foreign governments and international organizations by grant, credit, or cash sales, in furtherance of national policies and objectives.

Security assurance

The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance of their national contractors and citizens. It also includes a statement by a responsible official of a foreign government or international organization that the recipient of U.S. classified military information possesses the requisite security clearance. It also indicates that the original recipient is approved by his or her government for access to information of the security classification involved and that the recipient government will comply with security requirements specified by the United States.

Security manager

DA official designated to be responsible for supervising all security aspects of a classified meeting.

Security Policy Automation Network (SPAN)

A wide area computer network sponsored by the OUSD(P) consisting of a DOD-wide SECRET-high classified network and a separately supported unclassified network that supports communications and coordination among DOD activities on foreign disclosure, export control, and international arms control and cooperation subjects.

Sponsorship

- a.* In context of meeting, provision of DA resources (such as, personnel and funds) in support of the meeting.
- b.* In context of visit by foreign visitor to U.S. industry, DA authorization for disclosure of information on US Munitions List by a U.S. commercial firm, irrespective of whether the firm possesses a munitions license (that is, sponsorship of an exemption to the ITAR).
- c.* In context of visit by foreign representative, statement rendered by foreign government or international organization on behalf of foreign representative indicating that the latter's interaction with DA is officially sanctioned by the former, which assumes full responsibility for visitor's actions and for information that may be disclosed to visitor. (Also known as "security assurance".)

Standardization Representative (StanRep)

A StanRep is an operational FLO certified by the U.S. Army to represent the British, Canadian, or Australian government under the authority of the Basic Standardization Agreement. Each of the participating Armies provides StanReps to other Armies as desired to conduct liaison between the "parent" Army and the "host" Army in pursuit of ABCA goals and objectives.

Technical data package (TDP)

Technical description of item or service adequate for use in procurement. Description will be sufficiently complete to control configuration to required degree of design disclosure and item quality to required level. Package will consist of all applicable technical data, such as plans, drawings, and associated lists, specifications, purchase descriptions, standards, models, performance requirements, quality assurance provisions, and packing data.

Technical information/data

Knowledge including scientific knowledge that is in communicable form and relates to research, development, engineering, testing, evaluation, production, operation, use and maintenance of munitions (arms, ammunition, and implements of war), and other military supplies and equipment.

Technical data with military or space application

Technical data with military or space application is any blueprint, drawing, plan, instruction, computer software and documentation, or other technical information that can be used or be adapted to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

Technology Research and Development Project (TRDP)

International TRDP are collaborative efforts involving basic, exploratory, and advanced technologies.

Technology transfer

The process of cooperatively adapting existing DA R&D results, technology, or technical know-how to meet U.S. civilian needs, such as cooperative research and development agreement, or the transfer of defense article and services to foreign governments through FMS or DCS channels. Technology transfer is also the process of matching the solutions resulting from DA programs in the form of existing science and engineering knowledge and capabilities to the problems of industry or the public.

Third party

A third country or international organization other than the United States and second country or international organization.

Third party transfer

Transfer of United States defense articles, services, and training to a country (a third country) from a country that originally acquired such items from the United States. As a condition of the original sale or transfer, the recipient government must obtain the consent of the President of the United States for any proposed third country/party transfer.

Training

Formal or informal instruction of foreign nationals in the United States or overseas by—

- a.* Officers or employees of the United States, contract technicians, or contractors (including instruction at civilian institutions); or
- b.* Correspondence courses; technical, educational, or information publications and media of all kinds; training aids; orientation; training exercise; and military advice to foreign military units and forces (including their military and civilian personnel).

U.S. Army exchange personnel

Military or civilian officials of the U.S. Army who are assigned to a foreign defense establishment, according to the

terms of an applicable Exchange Agreement, and who perform duties, prescribed by a position description, for the foreign defense establishment.

U.S. person

A person who is a lawful permanent resident as defined by 8 USC 1101(a)(20) or who is a protected individual as defined by 8 USC 1324b(a)(30). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state or local) entity. It does not include any foreign person.

a. 8 USC 1101(a)(20) — The term “lawfully admitted for permanent residence” means the status of having been lawfully accorded the privilege of residing permanently in the United States as an immigrant according to the immigration laws, such status not having changed.

b. 8 USC 1324b(a)(30) — The term “protected individual” means an individual who— (A) is a citizen or national of the United States, or (B) is an alien who is lawfully admitted for permanent residence, is granted the status of an alien lawfully admitted for temporary residence under section 1160(a) or 1255a(a)(1) of this title, is admitted as a refugee under section 1157 of this title, or is granted asylum under section 1158 of this title; but does not include (i) an alien who fails to apply for naturalization within six months of the date the alien first becomes eligible (by virtue of period of lawful permanent residence) to apply for naturalization or, if later, within six months after November 6, 1986, and (ii) an alien who has applied on a timely basis, but has not been naturalized as a citizen within 2 years after the date of the application, unless the alien can establish that the alien is actively pursuing naturalization, except that time consumed in the Service’s processing the application will not be counted toward the 2-year period.

Visit authorization

There are three types of visit authorizations—

a. A ONE-TIME VISIT AUTHORIZATION permits contact by a foreign national with a DOD Component or DOD contractor facility for a single, short-term occasion (normally less than 30 days) for a specified purpose.

b. A RECURRING VISIT AUTHORIZATION permits intermittent visits by a foreign national to a DOD Component or DOD contractor facility over a specified period of time for a Government-approved license, contract or agreement, or other program when the information to be released has been defined and approved for release in advance by the USG.

c. An EXTENDED VISIT AUTHORIZATION permits a single visit by a foreign national for an extended period of time. Extended visit authorizations are to be used when a foreign national is required to be in continuous contact with a DOD Component or a DOD contractor facility beyond 30 days for one of the following situations:

- (1) Certification as a FLO or foreign exchange personnel (ESEP, MPEP, CPP) to a DA activity.
- (2) Training at a contractor facility under an FMS case, except for those individuals on ITOs. If it is in the Army’s interest, Army-sponsored training at a contractor or Army facility under DCS.
- (3) Assignment of a foreign contractor’s employees if the foreign contractor is under DA contract and performance on the contract requires assignment of the employees to the Army or Army activity at a contractor facility. This individual will be considered a FLO.

Section III

Special Abbreviations and Terms

This section contains no entries.

Index

Army Materiel Command (AMC), 1-7, 1-12, 4-2

Assistant Secretary of the Army (Acquisition, Logistics, and Technology),

delegated disclosure authority, 2-9

responsibilities, 1-9

TCP, 4-2

Chief of Engineers,

responsibilities, 1-7, 1-14

Classified military information, 2-3a

disclosure authority delegation, 2-8 through 2-10

disclosure authority re-delegation, 2-9k

disclosure authorities, 2-9

disclosure criteria, 2-6

disclosure, documentary, 3-4

administrative procedures, 3-8 through 3-10, Table 3-1

DTIC, 3-4c

disclosure, emergency, 2-9l

disclosure, international activities, Appendix I

disclosure levels (maximum delegated), 2-5

disclosure limitations, 2-6a(4)

disclosure, one-time, 2-9m

disclosure programs, 2-8

disclosure, visits, 3-1 through 3-3, Appendix J

Computers and Computer Networks, 3-5, Appendices K through O

NIPRNET, 3-7

SIPRNET, 3-6

Conferences (Meetings and Symposia), Appendix H

Contact officer, Appendices J through O

Contacts with foreign representatives, 1-4a(4)

Controlled unclassified information, 1-4e(10), 2-3b(1)

disclosure authority, 2-8

Cooperative Program Personnel (CPP), Appendix O

Delegation of disclosure authority letter (DDL), 2-10, Appendix E

Deputy Chief of Staff for Intelligence,

delegation of disclosure authority, 2-10

responsibilities, 1-6

role in disclosure, 2-12

TCP, 4-2

Deputy Chief of Staff for Logistics,

delegated disclosure authority, 2-9

responsibilities, 1-7

Deputy Chief of Staff for Operations and Plans,

delegated disclosure authority, 2-9

responsibilities, 1-8

Deputy Under Secretary of the Army for International Affairs,

delegated disclosure authority, 2-9

responsibilities, 1-5

TCP, 4-2

Deputy Under Secretary of the Army for Operations Research,

delegated disclosure authority, 2-9

responsibilities, 1-10

Director, Information Systems for Command, Control, Communications and Computers (DISC4),

delegated disclosure authority, 2-9

responsibilities, 1-14

TCP, 4-2

Disclosures (see Classified military information)

Eighth US Army, 1-16

Engineers and Scientists Exchange Program (ESEP), Appendix N
Exchange personnel, (see Military Personnel Exchange Program, and Engineers and Scientists Exchange Program)

False impressions, 2-2

FORDTIS, 3-10

Foreign disclosure officer, 2-11

Foreign liaison officer (FLO), Appendix K

Foreign test and evaluation, Appendix I

Frequently Asked Questions (FAQ), Appendix G

HQDA agency heads, 1-7

Imperatives of engagement, 2-1

International Visits Program, Appendix J

Major Commands (MACOMs), 1-7, 1-16

Management Control Evaluation Checklist, Appendix B

Meetings (see Conferences)

Military information,

 categorization, 2-3

 categories, 2-4

Military Personnel Exchange Program (MPEP), Appendix M

National Disclosure Policy Committee, 1-6b(1) and 1-6c

National Disclosure Policy,

 disclosure levels, 2-5

 exceptions (ENDPs), Appendix C

National Military Strategy, 2-1

National Security Strategy, 2-1

Official communications with foreign representatives

 Channels, 1-4a(3)

Overseas Army Activities (non-MACOMs), 1-17

Overseas MACOMs, 1-16

Policy, 1-4

 Definition, 1-4a(1) through 1-4a(3)

Program Protection Plan (PPP), 4-3c

Public domain information, 2-3b(2)

Security protection and assurances, 2-6a(2)

Standardization representative (StanRep), Appendix L

Summary Statement of Intent (SSOI), 4-3b, Appendix F

Technology Assessment/Control Plan (TA/CP), 4-3a, Appendix D

Technology Control Panel, 4-2

The Judge Advocate General,

 delegated disclosure authority, 2-9

 responsibilities, 1-7, 1-13

 TCP, 4-2

The Surgeon General,

 delegated disclosure authority, 2-9

 responsibilities, 1-7, 1-14

 TCP, 4-2

U.S. Army Criminal Investigation Command,

 responsibilities, 1-7, 1-15

U.S. Army Europe, 1-16

U.S. Army Intelligence and Security Command,

responsibilities, 1-7, 1-11
U.S. Army Pacific, 1-16
U.S. Army Southern Command, 1-16
US/Canada Joint Certification Program, Appendix J

UNCLASSIFIED

PIN 004070-000

USAPA

ELECTRONIC PUBLISHING SYSTEM

OneCol FORMATTER .WIN32 Version 142

PIN: 004070-000

DATE: 03- 8-01

TIME: 13:23:54

PAGES SET: 161

DATA FILE: R:\draftpubs\r380-10\Sgml\r380-10.fil

DOCUMENT: AR 380-10

DOC STATUS: REVISION