Army Regulation 380–10

Security

Foreign Disclosure and Contacts with Foreign Representatives

Headquarters
Department of the Army
Washington, DC
6 June 2003

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-10
Foreign Disclosure and Contacts with Foreign Representatives

This revision--

- Clarifies the province of foreign disclosure as governing the disclosure of classified military information to foreign governments and international organizations (para 1-4a).

- Assigns the Deputy Chief of Staff, G-2 with executing responsibilities for the Secretary of the Army as the principal foreign disclosure authority for the Army and with monitoring and coordinating technology protection issues (para 1-5).

- Assigns the Deputy Chief of Staff, G-2 the responsibility for providing foreign liaison and protocol support to the Army leadership, oversight of support to distinguished foreign visits to Headquarters, Department of the Army, and administrative support to foreign military attachés resident in Washington, DC (para 1-5).

- Assigns responsibility to organizations for the entry of all first-time disclosure decisions involving classified military information to foreign governments and international organizations into the Security Policy Automation Network (paras 1-5 through 1-14).

- Assigns disclosure authority to the Chief of Staff, Army; Vice Chief of Staff, Army; and Under Secretary of the Army for United States Army-originated classified military information according to the provisions of the National Disclosure Policy (para 2-8).

- Updates the delegated disclosure authority of Headquarters, Department of the Army principals (para 2-8).

- Delineates the role and responsibilities of foreign disclosure officers (paras 2-10, J-6, and K-6).

- Identifies the requirement for foreign disclosure officers to attend the Army Foreign Disclosure Certification Course (para 2-10b).

- Updates the requirements regarding delegation of disclosure authority letters in support of international programs and describes policy and use of position disclosure authority letters (app D).

- Clarifies the definition and requirements regarding recurring visit authorization (app I).

- Updates the policy and procedures involving requests for classified military information by foreign standardization representatives under the American, British, Canadian, and Australian Armies Standardization Program (app K).

Headquarters
Department of the Army
Washington, DC
6 June 2003

*Army Regulation 380–10

Effective 7 July 2003

Security

Foreign Disclosure 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 publication is a major revision.

Summary. The National Defense Strategy of the United States stresses that security cooperation is vital for our security. To achieve our defense objectives, the United States must remain the preferred partner for the community of States that shares our interests. Foreign disclosure is a key component that contributes to the achievement of our strategy of cooperation. This regulation provides policy and procedures for the disclosure of United States Army classified military information to foreign governments and international organizations; policy regarding contacts with foreign representatives; certification of foreign liaison officers 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 foreign disclosure involvement in 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 or protection processes.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this approval authority, in writing, to a division chief within the Office of the Deputy Chief of Staff, G–2.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated. The management control checklist is at appendix L.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2.

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 the Office of the Deputy Chief of Staff, G–2, ATTN: DAMI–CDD, 1000 Army Pentagon, Washington, DC 20310–1000.

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, dated 15 February 2001.

UNCLASSIFIED

Contents—Continued

Policy • 1–4, *page 1*

Section II
Responsibilities, page 4
Deputy Chief of Staff, G–2 • 1–5, *page 4*
Deputy Under Secretary of the Army (Operations Research) • 1–6, *page 4*
Assistant Secretary of the Army (Acquisition, Logistics, and Technology) • 1–7, *page 4*
Deputy Chief of Staff, G–3 • 1–8, *page 5*
The Judge Advocate General • 1–9, *page 6*
The Surgeon General, the Chief of Engineers, and the Chief Information Officer, G–6 • 1–10, *page 6*
Heads of Headquarters, Department of the Army field operating agencies and staff support agencies and commanders of major Army commands • 1–11, *page 6*
Commanding General, U.S. Army Materiel Command • 1–12, *page 6*
Commanding General, U.S. Army Intelligence and Security Command • 1–13, *page 7*
Commanding General, U.S. Army Criminal Investigation Command • 1–14, *page 7*
Commanders of major Army commands outside continental United States • 1–15, *page 7*
Other outside continental United States Army activities • 1–16, *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 Classified Military Information and Delegation of Disclosure Authority, page 12
Classified military information disclosure authority and delegation of authority • 2–8, *page 12*
Delegation of disclosure authority letter • 2–9, *page 13*
Responsibilities and establishment of foreign disclosure officers • 2–10, *page 14*
Foreign disclosure channels and general decision procedures • 2–11, *page 14*

Chapter 3
Modes, Methods, and Channels for Classified Military Information Disclosures and Related Administrative Procedures, *page 15*

Section I
Procedures for Disclosure to or by Visitor, Exchange, Cooperative, and Liaison Personnel, page 15
Concept • 3–1, *page 15*
Department of the Army classified military information disclosed during visits • 3–2, *page 15*
Department of the Army classified military information disclosed to foreign liaison officer personnel • 3–3, *page 16*
Documentary requests for United States classified military information • 3–4, *page 16*

Section II
Administrative Procedures, page 17
Concept • 3–5, *page 17*
Transmittal of classified military information documents and material to foreign governments and international organizations • 3–6, *page 17*
Recording classified military information disclosure determinations and transfers • 3–7, *page 17*

Contents—Continued

Foreign access to computers and computer networks • 3–8, *page 18*

Chapter 4
Technology Protection Program, *page 19*
Concept • 4–1, *page 19*
Technology Control Panel • 4–2, *page 19*
International technology transfer documentation • 4–3, *page 20*

Appendixes

A. References, *page 21*

B. Exceptions to the National Disclosure Policy, *page 25*

C. Technology Assessment/Control Plan, *page 29*

D. Delegation of Disclosure Authority Letter, *page 31*

E. Summary Statement of Intent, *page 38*

F. Frequently Asked Questions, *page 40*

G. Meetings, Conferences, and Symposia, *page 42*

H. Policy and Procedures for Disclosure of Classified Military Information in Support of International Activities, *page 43*

I. Department of the Army International Visits Program, *page 47*

J. Foreign Liaison Officers, *page 51*

K. Standardization Representatives, *page 66*

L. Management Control Checklist and Department of the Army Staff Assistance and Compliance Visits, *page 69*

Table List

Table 3–1: Document request procedures, *page 18*

Figure List

Figure 2–1: Political and military criteria, *page 11*
Figure B–1: Format for exception to National Disclosure Policy request, *page 26*
Figure B–1: Format for exception to National Disclosure Policy request—Continued, *page 27*
Figure B–1: Format for exception to National Disclosure Policy request—Continued, *page 28*
Figure C–1: Technology assessment/control plan format, *page 30*
Figure C–1: Technology assessment/control plan format—Continued, *page 31*
Figure D–1: Sample delegation of disclosure authority letter format for a weapon system, *page 34*
Figure D–1: Sample delegation of disclosure authority letter format for a weapon system—Continued, *page 35*
Figure D–2: Sample delegation of disclosure authority letter format for foreign liaison officers, foreign exchange personnel, and cooperative program personnel, *page 36*
Figure D–2: Sample delegation of disclosure authority letter format for foreign liaison officers, foreign exchange personnel, and cooperative program personnel—Continued, *page 37*
Figure D–2: Sample delegation of disclosure authority letter format for foreign liaison officers, foreign exchange personnel, and cooperative program personnel—Continued, *page 38*
Figure E–1: Summary statement of intent format, *page 39*
Figure E–1: Summary statement of intent format—Continued, *page 40*
Figure F–1: Frequently asked questions and corresponding answers, *page 41*
Figure J–1: Sample of certification form for security assistance foreign liaison officers, *page 57*
Figure J–1: Sample of certification form for security assistance foreign liaison officers—Continued, *page 58*
Figure J–2: Sample of generic certification form for operational foreign liaison officers, *page 59*
Figure J–2: Sample of generic certification form for operational foreign liaison officers—Continued, *page 60*
Figure J–2: Sample of generic certification form for operational foreign liaison officers—Continued, *page 61*

Contents—Continued

Figure J–3: Sample of certification form for specific operational foreign liaison officers, *page 62*
Figure J–3: Sample of certification form for specific operational foreign liaison officers—Continued, *page 63*
Figure J–4: Foreign liaison officer letter of offer and acceptance conditions and limitations, *page 64*
Figure J–4: Foreign liaison officer letter of offer and acceptance conditions and limitations—Continued, *page 65*
Figure K–1: Sample certification statement, *page 67*
Figure K–1: Sample certification statement—Continued, *page 68*
Figure K–1: Sample certification statement—Continued, *page 69*

Glossary

Index

Chapter 1
General

Section I
Introduction

1–1. Purpose
This regulation establishes policy and procedures and assigns responsibilities for the following: disclosure of Army classified military information (CMI) to foreign governments and international organizations; contacts with foreign representatives; certification of foreign liaison officers to Department of the Army (DA) commands, installations, and contractor facilities for which DA is the executive agent or has security cognizance; foreign representative attendance at Army-sponsored meetings, conferences, and symposia; and protection associated with the direct and indirect international transfer of critical military 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.

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 contacts with foreign representatives (see glossary), as outlined below.

(1) *Disclosure of classified military information.* 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), its departments or agencies, or departments or agencies 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, Volume 60, Federal Register. CMI may be in oral, visual, or documentary form. (See Army Regulation (AR) 380–5.)

(2) *Channels of official foreign disclosure communications.*

(a) On behalf of the Secretary of the Army and the Chief of Staff, Army (CSA), the Deputy Chief of Staff, G–2 (DCS, G–2) or his or her designee is the exclusive DA point of contact (POC) for foreign military attachés diplomatically accredited to the U.S. Government (USG) and for other representatives of foreign governments wishing to conduct official business with DA. In addition, the DCS, G–2 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 for U.S. Army information. All official foreign contacts with the Army in CONUS must be requested by diplomatically accredited military attachés or other properly authorized foreign embassy officials on behalf of their respective governments.

(b) Except as authorized by the DCS, G–2 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), 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 DCS, G–2 or his or her designated DCS, G–2 representative by their respective military attachés or other properly authorized foreign embassy officials. Except as required by AR 381–12, no report to Office of the Deputy Chief of Staff, G–2 (ODCS, G–2) of such unauthorized contact is necessary.

(c) All foreign national (see glossary) requests, regardless of the mode of transmittal (such as correspondence and e-mail), will be referred to the supporting Public Affairs Office for appropriate action. Except as required by AR 381–12, no report to ODCS, G–2 of such unauthorized contact is necessary.

(3) *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. DOD/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 Regulations (EAR).

(b) Foreign liaison officer. 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 (AR 614–10 and AR 70–41).

(d) Cooperative program personnel. Foreign government personnel assigned to an international program office hosted by DA or a foreign government pursuant to the terms of an International Cooperative Program 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 (AR 70–41).

(e) Meetings, conferences, and symposia. Attendance by foreign representatives at meetings, conferences, and symposia sponsored or hosted by DA.

b. This regulation designates specific DA officials to perform the tasks listed below.

(1) Authorize 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 cooperative program personnel (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—

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

(2) *National intelligence.* National and interdepartmental intelligence produced within the National Foreign Intelligence Board structure (AR 380–5).

(3) *Counterintelligence.* Counterintelligence operational information (AR 381–20).

(4) *Nuclear information.* Nuclear-related information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) (AR 380–5).

(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 (AR 380–40).

(7) *North Atlantic Treaty Organization 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 (AR 380–5 and AR 380–15).

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

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

(10) *Controlled unclassified information.* Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the USG. It includes U.S. information that is determined to be exempt from public disclosure according to DOD Directive (DODD) 5230.25 and DODD 5400.7 or that is subject to export controls according to Title 22, Code of Federal Regulations, parts 120–130 (22 CFR 120–130) (International Traffic in Arms Regulations (ITAR)) and 15 CFR 768 et seq. (Export Administration Regulations (EAR)). These types of information include but are not limited to: patent secrecy data, confidential medical records, inter- and intra-agency memoranda that are deliberative in nature, certain data complied for law enforcement purposes, data obtained from a company on a confidential basis, employee personal data, and internal rules and practices of a government agency that, 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

controlled unclassified information (CUI) under U.S. Army international cooperative programs. As such, this regulation does not cover such disclosures. CUI disclosures of this nature will be made according to governing regulations.

(11) *Classified military information to United States permanent resident aliens.* U.S. permanent resident aliens' access to CMI is governed by AR 380–5 (see glossary for definition of U.S. person).

(12) *Privacy Act information.* Information withheld from public disclosure under the Privacy Act (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 (such as Web sites) according to AR 360–1.

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

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

(16) *Proprietary information.* Classified or unclassified proprietary information, the rights to which are owned by private firms or citizens (such as patents, copyrights, and trade secrets). Disclosure cannot be made without the owner's consent, unless such disclosure is authorized by relevant legislation, and then release will be subject to such legislation.

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

(1) Non-government-to-government visits (AR 190–13).

(2) Training of foreign personnel under invitational travel orders (ITOs), including foreign students under a security assistance program, such as a foreign military sales (FMS) case or private individuals attending school at educational facilities under contract with the Army or any other governmental component (AR 12–15).

(3) Reciprocal exchanges of units for training purposes (AR 12–15).

(4) Cross-border movements of United States and Canadian forces (AR 525–16).

(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, a pertinent 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 (DOD 5220.22–M).

(6) Visits to U.S. Army or DA contractor facilities by foreign national employees of U.S. contractors (DOD 5220.22–M).

(7) Visits by foreign representatives or foreign nationals sponsored by another DOD or Federal agency (AR 190–13).

(8) Visits by foreign nationals, who are not representing their governments in an official capacity, to U.S. Army activities and DA contractor facilities (AR 190–13 or DOD 5220.22–M).

(9) Unclassified visits by Canadian government officials and certified Canadian contractors under the United States–Canada Joint Certification Program (according to ITAR).

(10) Visits for activities that are open to the public or hosted by the Public Affairs Office (AR 360–1 and AR 190–13).

(11) 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 Section 168, Title 10, United States Code (10 USC 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.

(12) Visits for social activities, international sporting events, official activities to which members of the public have been invited, authorized routine or emergency medical treatment, and transient purposes (such as brief stopovers on a flight). Such visits will involve the release of public domain information only (AR 190–13).

(13) Visits by foreign representatives or foreign nationals participating in the U.S. Department of State (for example, the U.S. Information Service) orientation tours (AR 190–13).

g. This regulation specifically prohibits the disclosure of CMI:

(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) 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. ODCS, G–2 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.

Section II
Responsibilities

1–5. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Execute responsibilities for the Secretary of the Army as the principal foreign disclosure authority for the Army and technology protection (that is, counterintelligence, intelligence, security, and foreign disclosure) support to the Technology Transfer Program. The management control checklist is provided at appendix L.

b. 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 identified for foreign disclosure. Such action will be taken 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, DODD 5230.20, DODD 2040.2, and DODD 5530.3. The DCS, G–2 will—

(1) Exercise exclusive approval authority for disclosure of DA CMI to foreign representatives.

(2) Exercise authority to delegate CMI disclosure authorization 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.

c. Provide an Army member to represent the Secretary of the Army to the National Disclosure Policy Committee (NDPC).

d. Coordinate, review, and submit all Army exceptions to NDP–1 (ENDPs) (see app B) requests.

e. Control internal distribution of NDP–1 and provide necessary delegated disclosure authority to implement NDPC records of action (RAs) (see glossary) throughout DA.

f. Be the primary POC for technology protection issues within HQDA (see chap 4). In this role, the DCS, G–2 will—

(1) Task appropriate HQDA elements to prepare technical assessments, as needed, identify critical program information (CPI) (see glossary) that is identified in documents such as the technology assessment and control plan (TA/CP) (see app C), and provide additional technology protection 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 protection implications.

(4) Ensure that appropriate protection measures are considered for each program that potentially involves the international transfer of CMI.

(5) Chair the technology control panel (TCP) (see para 4–2).

g. Ensure that all first-time disclosure decisions involving CMI are recorded in the Security Policy Automation Network (SPAN) in compliance with DOD Instruction (DODI) 5230.18.

h. Record decisions on foreign government requests for visit authorization to DA elements in the Foreign Visits System (FVS) in compliance with DODI 5230.18.

i. Administer, manage, and execute the foreign liaison officer (FLO) program.

j. Conduct oversight of the Army foreign disclosure training program.

k. Exercise exclusive authority over the approval of all Army delegation of disclosure authority letters (DDLs) (see app D).

l. Review all munitions license applications that are referred to HQDA for Army recommendations and involve the export of classified defense articles or data.

m. Provide protocol support to the Army leadership, oversight of support to distinguished foreign visits to HQDA, and administrative support to foreign military attachés resident in Washington, DC.

1–6. Deputy Under Secretary of the Army (Operations Research)

The Deputy Under Secretary of the Army (Operations Research) (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.

c. Ensure that all first-time disclosures or denials of CMI by the Office of the DUSA(OR) are recorded in SPAN.

1–7. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

The Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA(ALT)) will—

a. Identify critical U.S. military system-specific technologies.

b. Oversee the development, coordination, and implementation of policy and programs associated with the Army's security cooperation activities (that is, foreign military sales, foreign military training, allocation of excess defense articles to foreign countries, armaments cooperation, technology transfer, direct commercial sale, and munitions case processing).

c. Serve as the Secretary of the Army's single executive for providing export policy oversight and chairing and directing the Technology Transfer Security Assistance Review Panel, which serves as the executive decision authority for Army export control (to include foreign disclosure as it pertains to security cooperation).

d. Exercise direct tasking authority over the Army's designated executive agents for the execution of their delegated security cooperation responsibilities.

e. Administer and oversee research, development, test, evaluation, and acquisition programs, to include the execution of data/information exchange programs, cooperative research and development (R&D) memoranda of understanding, and participating in international forums concerning the aforementioned subjects.

f. Task preparation of and validate TA/CPs and summary statements of intent (SSOIs) (see app E).

g. Provide technical experts on DA, DOD, and interagency committees, panels, and working groups that address technology transfer and militarily critical technologies.

h. Provide an Army member to represent the Secretary of the Army to the DOD Arms Transfer Policy Review Group.

i. Ensure technology transfer security is considered for each Army program that potentially involves the international transfer of CMI.

j. With the ODCS, G–2 and The Judge Advocate General (TJAG), devise effective technical and contractual safeguards to prevent the inadvertent diversion of critical U.S. technology.

k. Have HQDA responsibility for formally coordinating the DOD Militarily Critical Technologies List (MCTL).

l. Coordinate and submit the Army position regarding munitions license requests for defense articles and services on the U.S. Munitions List as well as dual-use technologies on the Commerce Control List.

m. Oversee the U.S. Engineers and Scientists Exchange Program (ESEP) (AR 70–41).

n. Administer, manage, and execute the U.S. Army CPP Program (AR 70–41).

o. Provide a representative to the TCP.

p. Ensure foreign disclosure guidance on materiel items is provided to U.S. Army Training and Doctrine Command (TRADOC) FDO in sufficient detail to support training course development for foreign government trainees, as required.

q. Ensure that all first-time disclosures or denials of CMI by the Office of ASA(ALT) are recorded in SPAN.

1–8. Deputy Chief of Staff, G–3

The Deputy Chief of Staff, G–3 (DCS, G–3) will—

a. Serve as the Army Staff focal point to ensure the capability and application of total Army forces to execute national and military strategy worldwide and ensure that current and future Army strategy, planning guidance, and policy are reflected in force development requirements.

b. Provide HQDA with strategic analysis pertaining to national security issues involving international and regional arms control treaties, agreements, and policies.

c. Ensure that Army plans, policies, concepts, and doctrine conform to national, DOD, Joint Staff, and Army security policies and agreements as well as to multinational force compatibility agreements. Serve as Army Staff lead in developing and reviewing operational concepts for Army, Joint, and multinational operations, to include joint experimentation.

d. Serve as the principal advisor to the CSA on Joint matters, National Security Council matters, and the political/military aspects of international affairs.

e. Assess operational impact on U.S. forces if U.S. Army weapon systems were to be illegally transferred to U.S. adversaries.

f. Assess what, if any, impact a proposed weapon system transfer will have on U.S. military cooperation and operational plans and to what degree the system or item counters that country's military threat.

g. Ensure that the disclosure criteria cited in chapter 2 of this regulation are considered for each international program for which the DCS, G–3 has primary responsibility and which potentially involves the international transfer of CMI.

h. Assess implications of proposed disclosures/transfers on DCS, G–3 programs, plans, and policies.

i. Provide a representative to the TCP.

j. Administer, manage, and implement the U.S. Military Personnel Exchange Program (DOD term; U.S. Army term is Personnel Exchange Program (PEP)) (AR 614–10).

k. Oversee the American, British, Canadian, and Australian Armies standardization program, including the standardization representative (StanRep) (see glossary) program.

l. Formulate, establish, and disseminate operations security and physical security policy and procedures regarding access, badging, escorts, and vehicle decal identification of foreign visitors.

m. Oversee Latin America Cooperation activities.

n. Ensure that all first-time disclosures or denials of CMI by the Office of the DCS, G–3 (ODCS, G–3) are recorded in SPAN.

1–9. The Judge Advocate General

TJAG will—

a. Together with DCS, G–2 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 chairperson 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.

e. Ensure that all first-time disclosures or denials of CMI by the Office of TJAG are recorded in SPAN.

1–10. The Surgeon General, the Chief of Engineers, and the Chief Information Officer, G–6

The Surgeon General (TSG), Chief of Engineers (COE), and Chief Information Officer, G–6 (CIO/G–6) 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 CIO/G–6: Formulate, establish, and disseminate policy and procedures for access to computers and computer networks, to include foreign representatives and nationals.

d. Ensure that all first-time disclosures or denials of CMI by the Office of TSG, COE, and CIO/G–6 are recorded in SPAN.

1–11. Heads of Headquarters, Department of the Army field operating agencies and staff support agencies and commanders of major Army commands

Heads of HQDA field operating agencies and staff support 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 field operating agency and staff support agency. Designate, in writing, a single official to be the FDO for each MACOM.

c. 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 and this regulation.

(2) Ensure that all first-time disclosures or denials of CMI by the agency or command are recorded in SPAN.

d. Provide support to the Army international technology transfer program, as appropriate.

e. 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 10. A copy of all such reports will be provided to ODCS, G–2.

f. Appoint contact officers (see glossary), in writing, for all official foreign visitors to all echelons of their agency or command.

g. 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.

1–12. Commanding General, U.S. Army Materiel Command

The Commanding General, U.S. Army Materiel Command (CG, AMC) is responsible for the implementation of the Army's international cooperative R&D program. Specifically, the CG, AMC will—

a. Develop assessments to identify critical technologies developed in conjunction with R&D programs and identify and provide assessments of relative risks and benefits of international cooperation and the transfer of those technologies.

b. At ASA(ALT) direction, provide technical representatives and assistance to support DA and interagency working groups, committees, and panels on international technology transfer and critical technologies.

c. As directed by and in coordination with 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 international transfer.

d. 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.

e. Provide technical guidelines, recommendations, assistance, and data regarding control of technology transfer to foreign countries.

f. Coordinate intelligence assessments for all proposed international cooperative R&D programs.

g. Provide a representative to the TCP.

h. Ensure that all first-time disclosures or denials of CMI by AMC are recorded in SPAN.

1–13. Commanding General, U.S. Army Intelligence and Security Command

The Commanding General, U.S. Army Intelligence and Security Command (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, multidisciplined 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 suspected acts of espionage, unauthorized removal and retention of CMI, and known or suspected unauthorized disclosure of CMI, to include military technology and R&D data on acquisition systems.

e. Ensure that all first-time disclosures or denials of CMI by INSCOM are recorded in SPAN.

1–14. Commanding General, U.S. Army Criminal Investigation Command

The Commanding General, U.S. Army Criminal Investigation Command (CG, USACIDC) is responsible for investigating felony criminal cases that involve international technology transfer issues. The 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 DCS, G–2 of investigations regarding the illegal disclosure of CMI.

c. Serve as Army 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.

e. Ensure that all first-time disclosures or denials of CMI by USACIDC are recorded in SPAN.

1–15. Commanders of major Army commands outside continental United States

Outside continental United States (OCONUS) MACOM commanders will use the policy guidance contained in this regulation to establish local policies and procedures governing interactions with foreign representatives. For this purpose, OCONUS MACOMs are: U.S. Army Europe, U.S. Army Pacific, U.S. Army Southern Command, and Eighth U.S. Army. OCONUS MACOMs and Army component commands of unified commands are to adhere to unified command policies and procedures insofar as such policies and procedures are consistent with applicable DA guidance. ODCS, G–2 will be advised of any conflicts. Significant conflicts will be resolved at the DA/DOD level.

1–16. Other outside continental United States Army activities

Other OCONUS Army activities assigned to, or under the operational control of, an OCONUS MACOM commander will adhere to the OCONUS MACOM commanders' 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 Defense Strategy summary. The DOD has developed a new strategic framework to defend the nation and secure a viable peace. This framework is built around four defense policy goals: assuring allies and friends; dissuading future military competition; deterring threats and coercion against U.S. interests; and, if deterrence fails, decisively defeating any adversary. The presence of American forces overseas is a profound symbol of the U.S. commitment to its allies and friends. The U.S. military presence plays a critical role in assuring allies and friends that the nation will honor its obligations and is a reliable security partner. Through its willingness to use force in its own defense and that of others and to advance common goals, the U.S. demonstrates its resolve and steadiness of purpose and the credibility of the U.S. military to meet the nation's commitments and responsibilities. Toward these ends, the DOD promotes security cooperation with allies and friendly nations. A primary objective of U.S. security cooperation is to help allies

and friends create favorable balances of power in critical areas of the world to deter aggression or coercion. Security cooperation serves as an important means for linking DOD's strategic direction with those of U.S. allies and friends.

b. Role of foreign disclosure in United States National Defense Strategy. U.S. sharing of its military resources (such as CMI resident in technology and materiel) is a critical component of security cooperation. 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 nonallied 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. national security goals and objectives.

c. Classified military information disclosure support to National Defense 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 that 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 that result from either U.S. or combined initial planning and that may lead to the eventual disclosure of classified military materiel, technology, or information, including intelligence threat data or countermeasures information, must be authorized either by designated disclosure officials in the departments and agencies originating the information or by the NDPC.

2–3. Categorization of military information

a. Classified military information. 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.

(1) *Controlled unclassified information.* Unclassified information 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 complied 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. CUI disclosures will be according to governing statute, regulation, or policy.

(2) *Public domain.* For the purposes of this regulation, unclassified information that does not qualify for the status of CUI, as described in (1), above, is deemed to be actually or potentially in the public domain (in other words, suitable for disclosure to the public at large). 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.

(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 equipage, operation, maintenance, and support of its military forces or of 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 in this category. This category also includes information on 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, subsystem, 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 that 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 that 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, and so on) 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 that has completed acquisition milestone B or documentation used for production thereof, is 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 allow access/insight to classified algorithms or design rationale are considered to be manufacturing information. Unclassified software source code and software documentation that are required for minor software maintenance, interface/integration, or to make administrative changes to tables, symbols, markers, or displays will be handled through normal category 2 technology transfer channels.

(b) Build-to-print and assembly information. See (2)(a) and (2)(b), above.

(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 Air Defense Command).* North American Air Defense Command (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 United States/Canada defense agencies.

(b) U.S. operational and logistics plans for employment of reserve forces.

(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.

b. Unclassified information is not formally categorized, but the designations and descriptions above may be used as a baseline for disclosure decisionmaking.

2–5. Maximum delegated disclosure levels

NDP–1 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 the SPAN.

a. DA does not have the authority to authorize the disclosure of CMI that exceeds 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 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 ODCS, G–2, which reviews, coordinates, and submits the request to the NDPC. (See app B.)

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 1–7 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 ODCS, G–2, 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) *United States benefits.* Disclosures will result in benefits to the U.S. at least equivalent to the value of the information disclosed. For example:

(a) The United States 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 and Defense Intelligence Agency (DIA) Regulation 50–27.

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 on 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 United States.
e. The political benefits that could accrue to the United States.
f. Whether or not the transfer assists the United States in obtaining or securing base, transit, and over flight rights or access to strategic locations.
g. Other countries to which the United States has transferred the item.
h. The possible reaction of other countries in the region to the proposed sale.
i. Whether or not the United States 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 United States.
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 defensive capability.
d. How the transfer would increase the capability of friendly regional forces to provide regional security to assist the United States in the protection of strategic lines of communication.
e. How the transfer shall 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. Whether or not the country's technology base can 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.
l. Logistical support that will be required (maintenance, parts, instruction, personnel, changes, or updates).
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 may be 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, and so on.) If so, have proper approvals been obtained?
r. Will the disclosure of advanced technology, if compromised, constitute an unreasonable risk to the U.S. position in military technology and operational capabilities, regardless of the intended recipient?

Figure 2–1. Political and military criteria

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 Army may subsequently approve classified disclosures. DA officials responsible for reviewing, providing input on, 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 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), and so on) 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 nonbinding 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 nonbinding preliminary discussions should commence. If the decision is to commence nonbinding 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 all 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 ODCS, G–2.

Section II
Authority to Disclose Classified Military Information and Delegation of Disclosure Authority

2–8. Classified military information disclosure authority and delegation of authority

a. Under the provisions of NDP–1, the Secretary of the Army has been delegated the authority to disclose CMI originated by or for DA according to annex A and the policy statements of NDP–1. The Secretary of the Army hereby delegates the authority to disclose CMI originated by or for DA according to annex A and the policy statements of NDP–1 to the following principals: CSA, Under Secretary of the Army, VCSA, and DCS, G–2. The DCS, G–2 is the primary foreign disclosure authority within DA. All DDLs authorizing the disclosure of CMI originated by or for DA must be approved by the DCS, G–2 or his or her designee.

b. The Secretary of the Army hereby delegates to the HQDA officials identified below the authority to approve the disclosure of CMI for which they are the original classification authorities. This delegation of disclosure authority is limited to the categories, eligibility levels, and policy statements cited in NDP–1 and is provided for the implementation of approved Army international programs. In all cases, disclosure will be according to the provisions of NDP–1 and requires the written approval of both the original classification authority and the designated disclosure authority for the CMI in question. The DCS, G–2 may revoke or modify these delegations of disclosure authority as the DCS, G–2 deems appropriate.

(1) *Headquarters, Department of the Army delegated disclosure authorities.*

(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/interoperability (RSI) and have been approved according to AR 34–1, AR 550–51, or both.

1. DCS, G–3.

2. CIO/G–6.

3. 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. ASA(ALT).

2. TSG.

3. DCS, G–3.

4. CIO/G–6.

5. Deputy Chief of Staff, G–4.

(c) Category 3. Officials listed in the subparagraphs below have authority to make disclosure determinations for category 3 CMI (Applied R&D Information and Materiel). This authority applies within the substantive scope of international cooperative R&D agreements approved under 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. ASA(ALT).

2. DCS, G–3.

3. CIO/G–6.

(d) Category 4. Disclosures of category 4 CMI (Production Information) must be approved by ODCS, G–2 and the NDPC on a case-by-case basis.

(e) Category 5. The following officials have the 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. DCS, G–3.

2. TSG.

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

1. DCS, G–3.

2. Deputy Chief of Staff, G–1.

3. DCS, G–4.

(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 and DIA Regulation 50–27.

(2) *Security Policy Automation Network entries.* HQDA agency heads will ensure that all disclosures of CMI by their respective agencies are reported to ODCS, G–2 for recording into SPAN.

(3) *Delegated disclosure authority at MACOMs and below.* DCS, G–2 or his or her designee will issue DDLs to commands and agencies below HQDA, as required.

(4) *Redelegation.* Redelegation of the authority to disclose CMI is not authorized without specific written authorization from DCS, G–2 or his or her designee. Fully justified proposals regarding further delegation of disclosure authority will be submitted through command or agency channels to ODCS, G–2. If approval is granted, ODCS, G–2 will issue a DDL.

(5) *Emergency authority.* Under conditions of actual or imminent hostilities, MACOM commanders are delegated authority to disclose U.S. Army-originated CMI up to and including the SECRET level to an actively participating allied or coalition force when support of combined combat operations requires the disclosure of that information. ODCS, G–2, in cooperation with the Office of the Joint Chiefs of Staff 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 ODCS, G–2 of such disclosures at the earliest possible date.

2–9. Delegation of disclosure authority letter

A DDL is a document issued by the DCS, G–2 or his or her designee explaining classification levels, categories, scope, and limitations of information under Army's disclosure jurisdiction that may be disclosed to a foreign government or international organization representative. It is used to delegate authority to subordinate commands and agencies for the disclosure of CMI to foreign governments or international organizations in support of approved U.S. Army or DOD international programs. A DDL that authorizes the disclosure of CMI will be prepared collectively by the host DA command or agency proponent for the international activity involved, FDO, subject matter expert, and all other affected parties within the command or agency and then forwarded through command or agency channels to ODCS, G–2 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 program executive office (PEO) PM will be forwarded through PEO channels to OASA(ALT) for appropriate staffing. DCS, G–2 or his or her designee is the approval authority for all DDLs and revisions to DDLs. As a matter of policy, ODCS, G–2 will not approve blanket or overarching DDLs, such as organizational DDLs submitted by a MACOM that authorize disclosure authority for all or portions of its major subordinate commands (MSCs). However, DCS, G–2 or his or her designee grants local commanders and agency heads authority to approve DDLs that only

authorize the disclosure of unclassified information. Local FDOs may approve administrative modifications to DDLs, such as a change of contact officers or the expiration date of the document. DDLs are intended for internal Army use only and will not be provided to, nor will their contents be disclosed to, foreign representatives (see app D).

2–10. Responsibilities and establishment of foreign disclosure officers

An 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 and that routinely discloses U.S. CMI to foreign governments or international organizations in support of approved U.S. Army international programs. Note: Since the majority of official foreign government and international organization requests for U.S. information is submitted through foreign disclosure channels, FDOs will facilitate the administrative processing of all requests for information that are forwarded by ODCS, G–2 or through foreign disclosure channels and may eventually involve the disclosure of CUI.

a. Foreign disclosure officer appointments. FDO appointments will be in writing. Notification of such appointments will be made to MACOMs, which will provide ODCS, G–2 a consolidated FDO list no later than 15 January annually. FDOs or personnel within the security chain of command will not serve concurrently as contact officers for FLOs, foreign exchange personnel, or CPP participants.

b. Foreign disclosure officer training. All FDOs are required to attend the Foreign Disclosure Certification Course that is conducted by the U.S. Army Intelligence Center. Appendix F provides a reference list of frequently asked questions regarding foreign disclosure that all FDOs should be able to answer.

2–11. 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. Deputy Chief of Staff, G–2 role. DCS, G–2 or his or her designee is to receive and respond to all foreign disclosure requests for CMI. In the situations cited below, the DCS, G–2 or his or her designee has issued DDLs to 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 command or agency to which the individual is certified. That command or agency will render a response.

(3) A request by a certified British, Canadian, or Australian (BCA) Armies StanRep is to be addressed directly to the respective parent government national point of contact (NPOC), who oversees the topic of the requested information.

(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 OASA(ALT).

(5) Requests rendered in channels specified in certain approved international cooperative R&D agreements (for example, Defense Research, Development, Test and Evaluation Information Exchange Program agreements according to DODI 2015.4) are to be addressed by the proponent or originator of the international agreement.

(6) Requests addressed to OCONUS MACOM components of unified commands in channels specified in international agreements regarding combined planning and operations are processed by the Army component command.

(7) Requests through the Defense Technical Information Center (DTIC) are sent to the FDO of the command or agency originating the document. Commands and agencies that recommend denials of foreign government or international organization requests for classified documents through DTIC will refer their recommendations to ODCS, G–2 for final review and decision.

b. Foreign disclosure requests. 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 program responsibility, unless disclosure authority has been delegated.

c. Coordination and development of disclosure recommendations/decisions.

(1) Prior to rendering a decision on a recommendation or forwarding a recommendation to HQDA for a decision, if required, MACOMs and MSCs will coordinate with all affected DA organizations to develop a fully staffed and coordinated MACOM or DA position.

(2) Comments and recommendations on issues related to the disclosure of CMI will address the degree to which the disclosure request satisfies each of the basic disclosure criteria cited in paragraph 2–6. Additionally, the following considerations should assist commands or agencies in formulating their 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 1–4*e*(1) through 1–4*e*(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 that 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 data exchange annex (DEA); or Memorandum of Agreement or other international 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 ASA(ALT) 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 (for example, 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 Classified Military Information 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 cosponsored by DA elements. (See apps G through I for further details.)

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

(2) Certification of—

(a) FLOs, including StanReps, certified to DA (see apps J and K).

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

(c) Foreign representatives assigned to the DA workforce (AR 614–10 and AR 70–41).

(d) DA representatives assigned to the workforces 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. Department of the Army classified military information 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 the U.S. perspective only.

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

(1) *Official visits.* 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 I 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 DCS, G–2 or his or her designee approves the request. The DA host agency or command will transmit such notes in the manner prescribed for document disclosures in section II of this chapter. A receipt must be obtained for classified material provided to foreign representatives, regardless of its classification level. In all cases, the provisions of AR 380–5 and DOD 5220.22–M will apply.

(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 visitor's military attaché in the U.S. 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. Department of the Army classified military information disclosed to foreign liaison officer personnel

For information about DA CMI disclosed to FLO personnel, see paragraph 3–2. For detailed information about the Army FLO program, see appendix J.

3–4. Documentary requests for United States classified military information

Most disclosures of DA CMI occur through the direct personal interaction described in paragraphs 3–1 through 3–3. 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 ODCS, G–2 unless ODCS, G–2 has specifically authorized other channels to be used. 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 request 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 ODCS, G–2 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. Research and development. 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 the 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.

c. Defense Technical Information Center document requests. The 11 July 1990 Memorandum of Understanding (MOU) signed by the Departments of the 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, more than 50 foreign governments and international organizations have been granted DTIC accounts. Foreign government and international organization requests will be processed as follows:

(1) DTIC will send requests for CMI to the command or agency that originated the document.

(2) The FDO of that command or agency will coordinate the request with the originator or proponent of the classified document.

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

(4) If disclosure approval is decided and the command or agency has a DDL that covers the classified information resident in the requested document, the originator or proponent will sanitize (as required) and forward the document and DTIC Form 55 (Defense Technical Information Center Request for Release of Limited Document) through the FDO to DTIC.

(5) If denial is recommended or the command or agency has not been granted disclosure authority for the classified information resident in the requested document, the command or agency will forward the document and DTIC Form 55, with justification for denial or first-time disclosure, to ODCS, G–2 for final disclosure determination. Upon rendering a final decision, ODCS, G–2 will forward the document and the completed DTIC Form 55 to DTIC and make the appropriate entry in SPAN.

d. Other categories. Foreign government and international organization requests for documentary information regarding matters other than in *a* through *d*, above, 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 ODCS, G–2, 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) Command or agency is to obtain a copy of the document and review and complete Army coordination with all affected DA commands or agencies, as required. The commander or agency head will—

(a) If approving under a DDL issued by ODCS, G–2 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 II of this chapter. The FDO will notify ODCS, G–2 of the final decision.

(b) If it is not covered by an existing DDL, forward the document to ODCS, G–2 for action. Provide a recommendation and detailed justification.

(c) If denying the request, forward the document and justification for denial to ODCS, G–2 for a final decision.

(d) In all cases, ODCS, G–2 will administratively close the case.

(5) For requests involving proprietary data, return the request to the originating foreign embassy and inform the requesting embassy to submit the request to the owner of the proprietary data; forward the request to the owner of the proprietary data for action and provide a copy of the letter to the requesting embassy; or sanitize the proprietary data from the document (if it is not critical to the text) and render a decision or recommendation regarding the release of the sanitized data. The FDO will notify ODCS, G–2 of the action taken to close the case.

Section II
Administrative Procedures

3–5. Concept

Before DA CMI that has been approved for disclosure to a foreign government or international organization 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).

3–6. Transmittal of classified military information documents and material to foreign governments and international organizations

CMI that is transmitted in documentary or material form to recipient foreign governments and international organizations will be transmitted according to AR 380–5.

3–7. Recording classified military information disclosure determinations and transfers

The SPAN is an important database that records first-time disclosure decisions involving U.S. CMI to foreign governments and international organizations. The purpose of SPAN is to assist DA decisionmakers 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, SPAN can provide a tracking mechanism of the foreign disclosure of all U.S. Army CMI. It also can 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 actual first-time disclosures and all denials of U.S. CMI, SPAN can assist in reducing the foreign disclosure decision processing time. For example, if SPAN indicates that the CMI being requested

for disclosure to a specific foreign government or international organization has been previously disclosed to that foreign government or international organization, the disclosure decision process essentially ends, and the command or agency receiving the request may approve the disclosure of the requested CMI, provided there is justification for the release. In this case, no additional disclosure authority is required, and no additional entries into SPAN regarding the disclosure of the previously disclosed CMI to the identical foreign government or international organization are required. Therefore, if SPAN is to fulfill its purpose, the expeditious entry of all first-time disclosure decisions involving U.S. CMI is a critical administrative responsibility for all echelons of the U.S. Army.

a. SPAN is designed to record decisions regarding foreign disclosure of CMI. These include munitions licenses, strategic trade issues, ENDPs, visits by foreign representatives, certification of foreign representatives, and miscellaneous disclosure determinations (that is, all cases not related to the other five types).

b. All adjudications regarding foreign disclosure of CMI will be recorded in SPAN by the command or agency that actually disclosed the CMI or denied the request for CMI. The DA command or agency that makes the actual disclosure or denies the request is responsible for recording the data within 20 working days of the actual disclosure of CMI or denial decision.

c. DA agencies or commands having SPAN terminals will record the entry online. Those not having an online SPAN capability will make their entries through the Foreign Disclosure System (FDS), which has a Secret Internet Protocol Router Network (SIPRNET) interactive form to record the actual disclosure or denial. There is an offline version for those organizations without SIPRNET connectivity. The FDS entry will then be forwarded through organization foreign disclosure channels to the next higher echelon having a SPAN online capability.

3–8. Foreign access to computers and computer networks

The provisions of AR 380–19 will govern access by FLOs and other foreign officials assigned to U.S. Army organizations as well as official foreign government visitors to Army computer systems (stand-alone or network), to include the Non-Secure Internet Protocol Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET). Disclosure of CMI through U.S. Army computer systems to these foreign government officials will be according to the provisions of this regulation.

Table 3–1
Document request procedures

Item	If the information desired is	And the requester	And the 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 (for example, Army regulation, pamphlet, circular, field manual, and so on).	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 ODCS, G–2.
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 (for example, 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)

Table 3–1
Document request procedures—Continued

Item	If the information desired is	And the requester	And the information is	Then the requester must
6	Maps.	(N/A)	(N/A)	Acquire the information from the Defense Intelligence Agency, ATTN: COS–4, Washington, DC 20301–0001.
7	Contained in Military or Federal Standardization Documents (for example, 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 (for example, *ARMY Magazine*, *Infantry Magazine*, *Armor Magazine*, and so on).	(N/A)	(N/A)	Acquire the information directly from the publisher.
9	Under the auspices of a legally approved data or information exchange annex (DEA/IEA).	(N/A)	(N/A)	May acquire the information only via the appropriate technical project officer (TPO) or associate TPO (ATPO).
10	Other than those cited in Items 1–9.		(N/A)	Submit written request to ODCS, G–2.

Notes:

[1] Addresses for Government Printing Office (GPO) and National Technical Information Service (NTIS) are: Superintendent of Documents, Government Printing Office, 710 North Capital Street, NW, Washington, DC 20402–0001, and National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161–0001.

[2] Countries that are eligible to enter into FMS arrangements with the U.S. Army may be eligible to establish a FMS publications account with the U.S. Army Publishing Directorate (APD) for the purpose of obtaining Army administrative publications. Military attachés representing potentially eligible countries should inquire about the eligibility of their respective parent governments. For those eligible, the Army expects that such accounts will be established and maintained. The Director of Foreign Liaison will not provide administrative publication accounts with APD for foreign governments or international organizations.

[3] Other types of communications that are directly related to the actual or proposed acquisition of U.S. Army equipment and materiel under the auspices of FMS also may be referred directly to The Commander, U.S. Army Security Assistance Command, ATTN: DRSAC–SC, 5701 21st Street, Fort Belvoir, Virginia 22060–5940.

[4] Requests for documentary information that are to be submitted directly to USASAC are to be prepared according to the format and instructions depicted in the Military Attaché Guide provided to all embassies by HQDA.

[5] Requests originated by authorized foreign representatives of the customer country in the United States should be sent directly to USASAC or its designees.

Chapter 4
Technology Protection Program

4–1. Concept

This chapter describes the significance and the attention devoted to the Army technology protection program. The senior Army leadership recognizes the significance of international technology transfer in attaining our national security 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 the Army's critical technologies with the requirements to protect these technologies.

4–2. Technology Control Panel

a. Purpose of the Technology Control Panel.

(1) The DCS, G–2 has established the TCP as a coordinating mechanism to assist in carrying out the responsibility to manage and coordinate technology protection issues for the Army.

(2) The TCP is intended to facilitate rational and consistent nonroutine technology protection decisions based on comprehensive consideration of relevant factors.

b. Function of the Technology Control Panel. The TCP will—

(1) Develop and recommend Army technology protection policy to the ODCS, G–2 on a case-by-case basis.

(2) Ensure quality of control of Army technology protection actions.

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

c. Technology Control Panel composition.

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

(a) A representative of DCS, G–2 (chairperson).

(b) A representative of ASA(ALT).

(c) A representative of DCS, G–3.
(d) A representative of CIO/G–6.
(e) A representative of TSG.
(f) A representative of TJAG.
(g) A representative of TRADOC.
(h) A representative of Forces Command (FORSCOM).
(i) A representative of Space and Missile Defense Command (SMDC).
(j) 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. Technology Control Panel 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 ODCS, G–2 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 chairperson will convene a meeting of the TCP as required or at the request of one of the TCP members.

4–3. International technology transfer documentation

The following international technology transfer documents are essential parts of the Army's technology protection program:

a. Program protection plan. The program protection plan (PPP) is a DOD-mandated document required for acquisition programs. Development of PPP is the responsibility of the PM, in concert with the appropriate international cooperative program offices and foreign disclosure/security offices. The purpose of the PPP is to identify CPI 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 as soon as possible within the acquisition lifecycle. The PPP should be completed no later than milestone B. DODD 5200.39 and DA Pam 70–3 provide guidance regarding the development of the PPP.

b. Technology assessment/control plan. The TA/CP is another 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 (except international cooperative R&D 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 PPP and must be completed no later than milestone B. Format for a TA/CP is found at appendix C. 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 D.

c. Summary statement of intent. The SSOI is a DOD-mandated international cooperative programs document. It is required for all international cooperative R&D programs and replaces the TA/CP requirement for these programs. Development of SSOI is the responsibility of the PM, in concert with the appropriate international cooperative program offices and foreign disclosure/security offices. Format for an SSOI is found at appendix E. A DDL is required for all international cooperative R&D programs involving CMI and is forwarded as a companion document to the SSOI.

Appendix A
References

Section I
Required Publications

AR 380–5
Department of the Army Information Security Program. (Cited in paras 1–4*a*(1), 1–4*e*(2), 1–4*e*(4), 1–4*e*(7), 1–4*e*(11), 1–11*e*, 2–3*a*, 3–2*a*(3), 3–6, and G–1.)

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations. (Cited in paras 1–5*b* and D–2.) (Available at http://www.dtic.mil/whs/directives.)

DODD 5230.20
Visits, Assignments, and Exchanges of Foreign Nationals. (Cited in paras 1–5*b*, D–2, I–6, J–2*a*, J–2*b*, J–3*a*(1)(b)5, and J–3*a*(2)(b)5.) (Available at http://www.dtic.mil/whs/directives.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read a related reference to understand this publication. The United States Code is available at http://www.access.gpo.gov/congress/cong013.html. The Code of Federal Regulations is available at http://www.access.gpo.gov/nara/cfr.

AECA
Arms Export Control Act (22 USC 2778–2780). (Available at http://www.pmdtc.org/reference.htm.)

AR 5–11
Management of Army Models and Simulations

AR 11–31
Army International Activities 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)

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 Army Records Information Management System (ARIMS)

AR 34–1
International Military Rationalization, Standardization and Interoperability

AR 55–46
Travel Overseas

AR 70–1
Army Acquisition Policy

AR 70–26
Department of the Army Sponsorship of Unclassified Scientific or Technical Meetings

AR 70–31
Standards for Technical Reporting

AR 70–35
Research, Development, and Acquisition

AR 70–41
International Cooperative Research, Development, and Acquisition

AR 70–45
Scientific and Technical Information Program

AR 70–57
Military-Civilian Technology Transfer

AR 95–1
Flight Regulations

AR 190–13
The Army Physical Security Program

AR 210–7
Commercial Solicitation on Army Installations

AR 210–50
Housing Management

AR 340–21
The Army Privacy Program

AR 360–1
The Army Public Affairs Program

AR 380–15 (C)
Safeguarding Classified NATO Information (U). (Stocked and issued at the following address: ASNS–OPB, Room 1B889, 1000 Army Pentagon, Washington, DC 20310–1000.)

AR 380–19
Information Systems Security

AR 380–28 (C)
The Department of the Army Special Security System (U). (Available at www.dami.army.smil.mil/offices/dami-ch/daispom/reg.asp.)

AR 380–40 (O)
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (U). (Available at www.dami.army.smil.mil/offices/dami-ch/daispom/reg.asp.)

AR 380–67
The Department of the Army Personnel Security Program

AR 380–381
Special Access Programs (SAPS) (U)

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

AR 530–1
Operations Security (OPSEC)

AR 550–51
International Agreements

AR 614–10
U.S. Army Personnel Exchange Program With Armies of Other Nations; Short Title: Personnel Exchange Program.

DA Pam 70–3
Army Acquisition Procedures

DIA Regulation 50–27 (C)
Approval Procedures for Disclosure of Classified U.S. Intelligence to Senior Foreign Officials. (Available on the Secret Internet Protocol Router Network at http://www.dia.smil.mil/admin/REG–MAN/r50–27.)

DOD 5105.38–M
Security Assistance Management Manual. (Available at http://www.dtic.mil/whs/directives.)

DOD 5200.1–M
Acquisition Systems Protection Program. (Available at http://www.dtic.mil/whs/directives.)

DOD 5200.1–R
Information Security Program. (Available at http://www.dtic.mil/whs/directives.)

DOD 5220.22–M
National Industrial Security Program Operating Manual. (Available at http://www.dtic.mil/whs/directives.)

DOD 5230.18–M
Foreign Disclosure and Technical Information System (FORDTIS) User Manual. (Available at http://www.dtic.mil/whs/directives.)

DODD 2000.9
International Co-Production Projects and Agreements Between the United States and Other Countries or International Organizations. (Available at http://www.dtic.mil/whs/directives.)

DODD 2040.2
International Transfers of Technology, Goods, Services, and Munitions. (Available at http://www.dtic.mil/whs/directives.)

DODD 4500.54
Official Temporary Duty Travel Abroad. (Available at http://www.dtic.mil/whs/directives.)

DODD 5100.55
United States Security Authority for North Atlantic Treaty Organization Affairs. (Available at http://www.dtic.mil/whs/directives.)

DODD 5200.39
Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection. (Available at http://www.dtic.mil/whs/directives.)

DODD 5230.24
Distribution Statements on Technical Documents. (Available at http://www.dtic.mil/whs/directives.)

DODD 5230.25
Withholding of Unclassified Technical Data From Public Disclosure. (Available at http://www.dtic.mil/whs/directives.)

DODD 5400.7
DOD Freedom of Information Act (FOIA) Program. (Available at http://www.dtic.mil/whs/directives.)

DODD 5530.3
International Agreements. (Available at http://www.dtic.mil/whs/directives.)

DODI 2015.4
Defense Research, Development, Test and Evaluation (RDT&E) Information Exchange Program (IEP). (Available at http://www.dtic.mil/whs/directives.)

DODI 3200.14
Principles and Operational Parameters of the DOD Scientific and Technical Information Program. (Available at http://www.dtic.mil/whs/directives.)

DODI C–5220.29
Implementation of the North Atlantic Treaty Organization Industrial Security Procedures (U). (Available at http://www.dtic.mil/whs/directives.)

DODI 5230.18
Foreign Disclosure and Technical Information System (FORDTIS). (Available at http://www.dtic.mil/whs/directives.)

EAR
Export Administration Regulations (15 CFR 768 et seq.). (Available at http://www.bxa.doc.gov/policiesandregulations/index.htm.)

Executive Order 12958
Classified National Security Information (Volume 60, Federal Register, p. 19823). (Available at http://www.dtic.mil/dpmo/foia/eo12958.htm.)

ITAR
International Traffic in Arms Regulation (22 CFR 120–130). (Available at http://www.pmdtc.org/reference.htm.)

Military Attaché Guide
(Available at http://www.dami.army.pentagon.mil/offices/dami-fl/Attache-Guide.asp.)

MCTL
Militarily Critical Technologies List. (Available at http://www.dtic.mil/mctl.)

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 ODCS, G–2.)

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Form 11–2–R
Management Control Evaluation Certification Statement. (Available on the Army Electronic Library (AEL) CD–ROM (EM 0001) and the APD Web site (http://www.usapa.army.mil)).

DTIC Form 55
Defense Technical Information Center Request for Release of Limited Document. (Available at http://www.dtic.mil.)

Appendix B
Exceptions to the National Disclosure Policy

B–1. Exception to the National Disclosure Policy request

a. An ENDP request is required when a potential disclosure of CMI—

(1) Exceeds 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 ODCS, G–2, 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 and the intelligence community, respectively, and so on.

(2) Obtain HQDA staff concurrence in seeking the ENDP.

(3) Forward formal request for an ENDP to be initiated by ODCS, G–2.

Note. When possible, forward copy of completed draft of ENDP format through SIPRNET or by an attached 3½ disk.

c. DCS, G–2 or his or her designee will—

(1) Prepare the proposed ENDP in final form.

(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 an RA. DCS, G–2 or his or her designee will then effect dissemination of the decision, with accompanying disclosure guidance, to the HQDA proponent, the initiator of the request, the appropriate MACOM, and USASAC (if applicable), at a minimum.

B–2. Exception to the National Disclosure Policy request format

A sample format for an ENDP request is at figure B–1.

ODCS, G–2 (380–10)

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 2, Military Materiel and Munitions") 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 ODCS, G–2 as lead agency with initial requester (in other words, the 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 annex A. The writer is simply stating why an ENDP is needed.) ODCS, G–2 (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 toward the Government of (the recipient government). (Cite these policies or objectives, avoiding generalities such as "the recipient cooperates with the United States in pursuance of military or political objectives." ODCS, G–3 (lead); initial requestor and ODCS, G–2 (assist). The following political and military considerations should be addressed:

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 on 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 United States.

(5) (*) The political benefits that could accrue to the United States.

(6) (*) Whether or not the transfer helps the United States to obtain or secure base, transit, and overflight rights or access to strategic locations.

(7) (*) Other countries to which the United States has transferred the item.

(8) (*) The possible reaction of other countries in the region to the proposed sale.

(9) (*) Whether or not the United States 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 United States.

(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 defensive capability.

(4) (*) How the transfer would increase the capability of friendly regional forces to provide regional security to assist the United States in the protection of strategic lines 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) (*) Whether or not the country's technology base can 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.

Figure B–1. Format for exception to National Disclosure Policy request

(12) (*) Logistical support that will be required (maintenance, parts, instruction, personnel, changes, or updates).

b. (*) The military security of the United States 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 ODCS, G–2 (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 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 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. ODCS, G–2 (lead); OASA(ALT) (assist). This statement is supported in part by the following:

(1) (*) 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); ODCS, G–3 (assist).

(1) (*) (Is there a benefit 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); ODCS, G–3 and ODCS, G–2 (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. Initial requester (lead); OASA(ALT) and ODCS, G–2 (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 coproduction program or military sale when the United States 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); OASA(ALT) and ODCS, G–2 (assist).

Figure B–1. Format for exception to National Disclosure Policy request—Continued

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 correspondence that provides its 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.) ODCS, G–3 (lead); ODCS, G–2 (assist).

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.) Initial requestor (lead); OASA(ALT), and ODCS, G–2 (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 opposing the disclosure (usually involving the security status of the proposed recipient or concerns for the technology involved). 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 requester (lead); ODCS, G–3 and OASA(ALT) (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 requester (lead); OASA(ALT) and ODCS, G–2 (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 ODCS, G–3 and ODCS, G–2 action officers 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) of the 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 B–1. Format for exception to National Disclosure Policy request—Continued

Appendix C
Technology Assessment/Control Plan

C–1. Overview

DODD 5530.3, DOD 5200.1–M, AR 550–51, and DA Pam 70–3 set forth the requirements for the development of a TA/CP in support of either an international agreement or a foreign government or international organization involvement in an Army acquisition program.

C–2. Technology assessment/control plan development

In developing the TA/CP (see fig C–1), cognizant DA activities will consider and incorporate, as appropriate, all applicable NDP–1 and DOD technology transfer policy guidelines as well as Army disclosure policies. The FDO will assist the sponsor of the international agreement in the development of the TA/CP by providing applicable NDP–1 guidance for incorporation into the document.

a. 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.

b. DODD 5530.3, DOD 5200.1–M, AR 550–51, and DA Pam 70–3 also require that the cognizant DA activity develop a DDL (see app D) in conjunction with the TA/CP as part of a request for authority to conclude an agreement. The DDL will provide detailed guidance regarding disclosures of all elements of the system, information, or technology in question. Until the DDL is approved, there can be no promise or actual disclosure of sensitive information or technology. An SSOI (see app E) replaces the TA/CP requirement for all international cooperative R&D programs. For phased international cooperative R&D programs, the SSOI and DDL should address time-phased disclosures of technical data to ensure that sensitive information is protected from premature or unnecessary exposure.

c. Upon conclusion of the international agreement, the TA/CP or SSOI and the DDL will be updated (as required) to ensure that transfers of defense articles and information by USG or U.S. industry personnel comply with the established agreement, NDP–1, and applicable DOD/Army security policies and procedures.

1. 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.

2. 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 United States 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.

3. Technology Assessment.

a. Identify products or technologies involved in the program. This section of the assessment should discuss topics listed below using the Militarily Critical Technologies List and other applicable DOD/Service technology transfer policies as guides. The intelligence and security officers are the PM's link to the intelligence community for threat, foreign disclosure, 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) 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.

(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 to 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 whose loss 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, and so on).

(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.)

Figure C–1. Technology assessment/control plan format

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 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 United States).

(b) Their past record of compliance with such agreements and in protecting sensitive/classified information and technology.

4. 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 for the implementation of 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.

(2) Procedures to control disclosures by U.S. personnel at foreign facilities.

e. Other legal or proprietary limitations on access to and licensed uses of the technology in implementing technical assistance agreements.

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, coproduction, and information exchange programs.

c. The TA/CP is a "living" document, subject to continuous review and appropriate update. A product improvement proposal 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.

Figure C–1. Technology assessment/control plan format—Continued

Appendix D
Delegation of Disclosure Authority Letter

D–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. DCS, G–2 or his or her designee approves and issues DDLs for classified programs or projects regarding the following:

a. International agreements.

b. FLOs.

c. Army personnel exchange programs (PEP, ESEP, and CPPs).

d. Weapon systems.

e. Organizations.

f. Cooperative R&D (that is, DEAs, technology R&D programs (TRDPs), etc.).

D–2. Requirement

According to DODDs 5530.3, 5230.11 and 5230.20 as well as DOD 5200.1–M, AR 550–51, and DA Pam 70–3, a DDL is required for all U.S. Army weapons acquisition programs, international agreements, and FLO, StanRep, military personnel exchange program (MPEP), ESEP, and CPP positions. This requirement applies to the above-mentioned international programs regardless of whether access to CMI is involved. An approved DDL is required to be in place prior to a commitment to assign a FLO, foreign exchange program, or CPP participant to a DA component. In those cases where a DDL only authorizes the disclosure of unclassified information, the local commander or agency head may approve the DDL, but a hardcopy version of the document must be furnished to ODCS, G–2 within 10 working days of approval and signature. If the local commander or agency head exercises his or her authority to approve a DDL that only authorizes the disclosure of unclassified information, the organization may assign a case number to the DDL. An example of an appropriate case number would be "F–TRADOC–GH–001," which represents the program identification (F=operational FLO, S=security assistance FLO, M=MPEP, E=ESEP, or C=CPP), MACOM, two-letter foreign country code, and number.

D–3. Position delegation of disclosure authority letters

a. Position delegation of disclosure authority letters. Position DDLs may be established to facilitate the assignment of foreign representatives to DA organizations by reducing the processing time necessary to obtain approval of the supporting DDL. Position DDLs will support assignment positions that will not likely change over time. These positions usually apply to the assignment of FLOs to DA organizations.

b. Position delegation of disclosure authority letters that authorize the disclosure of classified military information. When a DA host organization conducts a review of a foreign representative assignment position at least 90 days prior to the scheduled departure of the incumbent and revalidates the position, the DA host organization may recommend revalidation of the existing DDL for the replacement person. (See app J regarding cases where the DA host organization recommends major modifications to or termination of the position.) For its part, when the DA host organization approves the RVA submitted by the replacement person's parent embassy in Washington, DC, DCS, G–2 or his or her designee will simultaneously approve the revalidation of the existing position DDL. Upon approval of the DCS, G–2 or his or her designee, the DA host organization will effect all applicable administrative modifications to the DDL, such as the case number (see para D–4 for additional information) and expiration date.

c. Position delegation of disclosure authority letters that only authorize the disclosure of unclassified information. When a DA host organization conducts a review of a foreign representative assignment position at least 90 days prior to the scheduled departure of the incumbent and revalidates the position, the local commander or agency head may exercise his or her authority to approve the supporting DDL provided it only authorizes the disclosure of unclassified information (see para D–4). The local commander or agency head may also approve modifications to the DDL only if unclassified information remains authorized for disclosure and the changes to the position description have been approved by the HQDA proponent for the international program. (See app J regarding cases where the DA host organization recommends termination of the position.) A copy of the approved DDL will be provided to ODCS, G–2 according to the procedures cited in paragraph D–4. Upon receipt of the approved DDL, the DCS, G–2 or his or her designee will then render a decision regarding the RVA submitted by the replacement person's parent embassy in Washington, DC, for the placement of the replacement official.

D–4. Preparation of delegation of disclosure authority letters

The command or agency that desires delegated disclosure authority will prepare the DDL for approval. As early as possible in the process, the supporting command or agency FDO will assist and guide, to include coordination with external organizations, the development of the DDL. The FDO will also be responsible for ensuring that all pertinent disclosure questions regarding the supported international program are raised and answered. Upon approval, the DDL will be the authority by which the FDO will render disclosure recommendations or decisions in support of the Army international program, provided the FDO is identified in paragraph(s) 4 and/or 7 of the DDL as a disclosure authority for that DDL. Upon receipt of approved DDL, the command or agency FDO should effect internal Army dissemination of the DDL to all affected parties, such as contact officers, PMs, subject matter experts, USASAC, training and doctrine elements, and operational units with that weapon system in their inventory.

D–5. Warning statement

The data elements contained in the following sample formats (see figs D–1 and D–2) must be used by DA elements to develop a DDL. From an administrative perspective, each DDL requires a warning statement stipulating that the DDL is an internal U.S. Army document that is not to be divulged, in total or in part (except para 5, which may be used in the Certification Statement form for FLO, PEP, ESEP, and CPP participants to describe the purpose of their assignments to a DA organization or agency), 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 that it clearly stands out. Examples of the wording of a warning statement are cited in the sample formats (see figs D–1 and D–2).

THE INFORMATION CONTAINED IN OR A COPY OF
THIS DDL WILL NOT BE DISCLOSED TO ANY
FOREIGN GOVERNMENT OR FOREIGN REPRESENTATIVE

(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 (Name of Weapon System)

1. CLASSIFICATION. The highest level of classified military information (CMI) that may be disclosed is (indicate highest security classification level authorized for disclosure: CONFIDENTIAL, SECRET, or TOP SECRET).

2. DISCLOSURE METHODS. Indicate types of disclosure methods authorized (for example, oral, visual, and/or documentary).

3. CATEGORIES PERMITTED. Indicate the categories of CMI authorized for disclosure (use chapter 2 of this regulation).

4. SCOPE. The Governments of X, Y, and Z.
Indicate clearly to whom the disclosure authority is granted and for what system. For example, "The Commander, U.S. Army Aviation and Missile Command, through the supporting FDO, is delegated authority to disclose CMI originated by U.S. Army Aviation and Missile Command 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 also may disclose CMI originated outside of U.S. Army Aviation and Missile Command 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.

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.

Clearly state what information under the cognizance of the disclosure authority is 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 (SCG). The SCG for a weapon system or technology provides a common language and framework for developing paragraphs 5 and 6. It is recommended that both the language and the topical subdivisions in the guides be used as a template for structuring paragraphs 5 and 6. For example:

Phase I—Foreign Customer Decision Phase. This phase covers preliminary discussions with prospective customers regarding end items sales, coproduction, and coassembly through FMS and/or DCS. A presale information package includes all information necessary for a prospective customer to make a purchase decision regarding a specific U.S. Army weapon system. This package should address and may include information, such as general weapon system performance characteristics and capabilities, technical specifications, price and availability (P&A) data, maintenance, and training. Preliminary disclosures are generally limited to the CONFIDENTIAL security classification level.

Phase II—Foreign Customer Decision to Buy Phase. This phase begins upon receipt of a commitment to buy, a signed contract, or a signed MOU. A postdecision 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 at the SECRET classification level, such as specific weapon system performance characteristics and capabilities, technical specifications, maintenance (organizational, intermediate, or depot) and training, DCS procedures and disclosure guidance, software, and so on.

Figure D–1. Sample delegation of disclosure authority letter format for a weapon system

6. NOT AUTHORIZED FOR DISCLOSURE. While disclosures of CMI are generally inclusionary, not exclusionary, with regard to the weapon system purchased, there is 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 protection of the CPI identified in the U.S. Army weapon system. In addition, CPI that was leveraged from another U.S. Army weapon system must be coordinated with the appropriate PM and protected accordingly. At a minimum, the information below should be included.

The following CMI is not authorized for disclosure under the terms of this DDL:

a. General.

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

(2) Electromagnetic signatures (if applicable to a 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) Noncooperative target 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 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 the foreign 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 that may be requested by a FLO or his government. Transfer of classified documents to foreign government representatives will be processed through government-to-government channels.

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 officials (identify) will record the disclosure (using the SPAN) 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.

(2) The authorized disclosing representative will ensure that all disclosures fitting any of the above categories and the terms of this DDL are recorded in the SPAN.

(3) The office responsible for the SPAN will enter the disclosure decision into the database.

(4) If a SPAN terminal is not available, the organization will use the FDS to record the first-time disclosure or denial and forward the entry to the next echelon possessing a SPAN online capability for recording in SPAN.

d. Regarding automation, the provisions of AR 380–19 will apply.

8. REDELEGATION. Redelegation of the authority vested in this DDL is not authorized without the written approval of the DCS, G–2 or his or her designee.

THE INFORMATION CONTAINED IN OR A COPY OF
THIS DDL WILL NOT BE DISCLOSED TO ANY
FOREIGN GOVERNMENT OR FOREIGN REPRESENTATIVE

Figure D–1. Sample delegation of disclosure authority letter format for a weapon system—Continued

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

(Office symbol) (380–10)

RVA START DATE: 01/01/99
RVA EXPIRATION DATE: 01/01/99
DDL APPROVAL NUMBER: F–AMC–GH–001
DDL APPROVAL DATE: 01/01/99
DDL EXPIRATION DATE: This DDL will be in effect indefinitely or until the scope is changed.
(If it is not a position DDL, expiration date will be scheduled departure date of the foreign representative.)

SUBJECT: Delegation of Disclosure Authority for Security Assistance Foreign Liaison Officer (FLO) of the Government of (country) (Identify case code by position and country, such as F–AMC–GH–case number.)

1. CLASSIFICATION. The highest level of classified military information (CMI) may be disclosed is (indicate highest security classification level authorized for disclosure: CONFIDENTIAL, SECRET, or TOP SECRET).

2. DISCLOSURE METHODS. Indicate types of disclosure methods authorized (for example, oral, visual, and/or documentary).

3. CATEGORIES PERMITTED. Indicate the category or categories of information authorized for disclosure (using chapter 2 of this regulation).

4. SCOPE. Indicate clearly to whom the disclosure authority is granted, for what program, system, study, and so on, and clearly indicate the authorized recipient(s). Indicate which agreements, MOUs, DEAs, FMS cases, international cooperative programs, installations, and/or agencies the individual(s) will, in the normal course of duties, deal with for the duration of his or her tenure in this position. For example: The Commander, U.S. Army Aviation and Missile Command, through the supporting foreign disclosure officer (FDO), is delegated authority to disclose CMI within the categories listed in paragraph 3. The Commander also may disclose CMI originated outside of U.S. Army Aviation and Missile Command when the disclosure is authorized in writing by the originator of the CMI and the originator has delegated disclosure authority for that CMI, and the information is within the scope of this DDL:

a. Government of (country) liaison officer (identify), (name of program).

b. Assigned To: U.S. Army Aviation and Missile Command (the command/agency to which the extended visit is authorized).

c. Associated Installations/Agencies/Commands: (for example, 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.)

d. 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.

5. AUTHORIZED FOR DISCLOSURE. In this paragraph, the identification (in other words, 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, and so on. This paragraph should provide specific details as to the body of CMI that the individual is required to 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.

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:

Figure D–2. Sample delegation of disclosure authority letter format for foreign liaison officers, foreign exchange personnel, and cooperative program personnel

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 ODCS, G–2.

a. General.

(1) Intelligence or threat information marked "not releasable to foreign nationals" (NOFORN).

(2) Restricted data or formerly restricted data.

(3) Information under the cognizance of another military department.

(4) Proprietary information owned by a private firm or citizen.

(5) Information obtained from a foreign government.

(6) Data that carries any caveats or markings, which limit access.

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

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

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

(10) Low observable requirements or advanced signatures data.

(11) Noncooperative target recognition data.

(12) 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 should provide procedures for disclosure of CMI not under the cognizance of the disclosure authority listed in this DDL.

7. PROCEDURES. The information below (at a minimum) must be included in this paragraph.

The following procedures will be used 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 the foreign 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 that may be requested by a FLO or his government. Transfer of classified documents to foreign government representatives will be processed through government-to-government channels.

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 officials (identify) will record the disclosure (using the SPAN) when one of the following occurs:

(a) First-time disclosure decisions 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.

(2) The authorized disclosing representative will ensure that all disclosures fitting any of the above categories and the terms of this DDL are recorded in the SPAN.

(3) The office responsible for the SPAN will enter the disclosure decision into the database.

(4) If a SPAN terminal is not available, the organization will use the FDS to record the first-time disclosure or denial and forward the entry to the next echelon possessing a SPAN online capability for recording in SPAN.

d. Regarding automation, the provisions of AR 380–19 will apply.

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. 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.

Figure D–2. Sample delegation of disclosure authority letter format for foreign liaison officers, foreign exchange personnel, and cooperative program personnel—Continued

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, and the approval of the DCS, G–2 or his or her designee.

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 that 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.

9. REDELEGATION. Redelegation of the authority vested in this DDL is not authorized without the written approval of the DCS, G–2 or his or her designee.

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

Figure D–2. Sample delegation of disclosure authority letter format for foreign liaison officers, foreign exchange personnel, and cooperative program personnel—Continued

Appendix E
Summary Statement of Intent

E–1. Concept

The SSOI is a DOD-mandated document that is required in support of proposed international cooperative R&D agreements. The FDO supporting the command or agency that sponsors the international cooperative R&D initiative is responsible for assisting in the development of the SSOI, specifically the information required in the security paragraph, as well as the accompanying DDL.

E–2. Summary statement of intent format

The format for the SSOI is provided at figure E–1.

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

Short title of proposed project:
DOD proponent:
Country/countries involved:

1. 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 that is necessary to develop new defense equipment or munitions, or what existing military equipment would be modified to meet U.S. requirements?

2. 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.

3. 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.

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

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

6. Benefits/Risks to the United States. List the advantages and disadvantages of this cooperative project. Address project timing, developmental and life cycle costs, technology to be shared and obtained, and impact on U.S. and foreign military capabilities to include Multinational Force Compatibility and Standardization 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 United States or an allied nation? If so, could that project satisfy or be modified in scope to satisfy the U.S. requirement?

7. 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 United States? 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)?

8. 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 nonfinancial contributions included in the cost shares.

c. If not equitable financially, justify on a program basis (show relative benefit to the DOD). 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.

Figure E–1. Summary statement of intent format

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.

9. 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?

10. Information Security and Technology Issues.

a. Briefly identify the products and/or technologies involved in the program and their NDPC category and classification. The Militarily Critical Technologies List may be used as a guide.

b. Have all of the requirements of the National Disclosure Policy been met, to include the need for an ENDP? The U.S. technical project officer for the proposed international agreement should contact his or her local FDO for this determination. If an ENDP is required, the request and supporting documentation must be prepared and staffed with the assistance of the local FDO through command channels to the HQDA proponent for appropriate coordination and submission to the NDPC. Do not state in this document whether or not an ENDP is required.

c. If known, describe the foreign availability of comparable systems and technologies and whether the U.S. technology has been shared through other programs (for example, foreign military sales or data exchange annex).

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 (for example, negating primary U.S. technological advantage(s), revealing U.S. system weaknesses, development of countermeasures, susceptibility to reverse engineering).

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 or controlled unclassified 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 (for example, 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.

11. 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 Request for Authority to Develop review period.

Figure E–1. Summary statement of intent format—Continued

Appendix F
Frequently Asked Questions

F–1. Concept

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

F–2. Frequently asked questions and corresponding answers

A list of frequently asked questions and corresponding answers is available at figure F–1.

Question: What is proprietary information?
Answer: See paragraph 1–4*e*(17).

Question: Which officials have the authority to approve DDLs?
Answer: See paragraph 2–9.

Question: May a FLO have access to a DDL?
Answer: See paragraph 2–9.

Question: Under a DDL, may an FDO 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 paragraph 2–11 for HQDA agency heads and the specific DDLs for MACOM commanders and major subordinate command commanders, as applicable.

Question: Can a PEO PM have delegated disclosure authority under a DDL?
Answer: Yes, provided the PEO PM has original classification authority for the information resident in his or her program.

Question: Which AR governs access to computer by a foreign government representative?
Answer: AR 380–19.

Question: Why is recording the first-time disclosures of CMI in the SPAN important?
Answer: See paragraph 3–7.

Question: Should DDLs be disseminated outside of FDO channels?
Answer: See paragraph D–1*c*.

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 paragraph 1–4*f*. 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, the disclosure of CMI is not an issue. Private citizens, such as foreign national employees and foreign students, who are working under a DA contract will 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 paragraphs I–7 and I–10.

Question: Is an 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 paragraph 1–4*f*.

Question: Can U.S. contractors serve as FDOs?
Answer: See paragraph 2–10.

Question: What does the command do if a FLO does not sign the certification statement form?
Answer: See paragraph J–2*c*(3).

Question: Can a FLO be simultaneously certified to more than one organization?
Answer: See paragraph J–2*c*(1).

Question: When is an RVA required for a FLO to visit U.S. Army or DOD commands or agencies?
Answer: See paragraph J–5*a*(2).

Question: In exchange programs, a participant may require access to U.S. Army computer systems. Which AR has authority over the granting of this access to U.S. Army computer systems for the participant who is working for the U.S. Army?
Answer: AR 380–19.

Figure F–1. Frequently asked questions and corresponding answers

Appendix G
Meetings, Conferences, and Symposia

Section I
Introduction

G–1. Approval policies

AR 380–5 governs Army policy related to the approval of, planning for, and conduct of meetings, conferences, and symposia (hereafter: "meetings") that are sponsored, cosponsored, or hosted by U.S. Army commands or agencies. This regulation addresses the foreign disclosure aspects of meetings that involve the attendance or participation of foreign representatives. With the exception of in-house meetings (see glossary), attendance or participation by foreign representatives at 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 when deemed in the best interests of the Army.

G–2. Types of meetings

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

Section II
Acquisition-Related Meetings

G–3. Rationalization/standardization/interoperability

RSI considerations and bilateral agreements promoting industrial cooperation have resulted in DA's adoption of policies (AR 34–1) that effectively increase 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).

G–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 necessitate early consideration of foreign disclosure issues. The procuring contracting officer is responsible for obtaining an Army position on foreign participation. This position must address which foreign nations may be eligible to receive the information to be disclosed during the performance of the contract. Successful foreign participation in cooperative developmental contracts, either as a prime contractor or a subcontractor, may require the disclosure of CMI. Therefore, Army PMs or item managers must involve their FDO in this process prior to advertising in the Federal Business Opportunities publication or any other announcement media and must consider such issues as—

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

b. The time and costs that must be factored into a contract to allow for the approval process for munitions licensing. Documentary transfer of classified deliverables (for example, interim reports and final reports) from U.S. contractor team members to foreign participants can be a lengthy process. If it is not considered prior to the 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. Participation consistent with applicable

U.S. laws, regulations, and security requirements in Army procurement initiatives by contractors from countries with which the DOD has agreements that encourage reciprocal participation in defense procurement may include access to U.S. CMI consistent with this regulation as follows:

(1) *Access to technical data.* Qualified government and industry representatives from those countries will be given appropriate access to the technical data, consistent with this regulation and the ITAR, necessary to bid on Army contracts.

(2) *Disclosure decisions.* Disclosure decisions involving those countries will be made prior to the announcement of the procurement, and the announcement will describe any restrictions on foreign participation.

(3) *Participation as subcontractor.* When it is determined that foreign contractors are not authorized to participate in the classified or other sensitive aspects of a potential contract, consideration should be given to their requests for participation in unclassified or less-sensitive aspects of the contract as a subcontractor.

(4) *Requests for documentation.* Requests by foreign entities for classified documentation must be submitted through government channels.

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

G–5. Procedures

After making a preliminary determination to convene or sponsor an acquisition-related meeting that may involve attendance or participation by 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.

(1) Commanders or agency heads may exercise their delegated visit authority to approve foreign representative visits to this type of meeting without the requirement for an RVA (see app I).

(2) The U.S. sponsor will notify all participants that presentations must be approved for release to the public. Criteria for approval and procedures for obtaining such approval are contained in AR 70–31 and AR 360–1. 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 EAR, as applicable, governs presentations by non-USG personnel when the information in question is not derived from a DOD contract.

b. Unclassified meeting closed to the public.

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

Note. According to AR 70–31 and subject to ITAR limitations, Canadian citizens may be certified by the Joint Certification Office.

(2) Coordination will be effected with all DA commands or agencies that may have a substantive interest in the subject matter of the meeting to establish foreign government or international organization attendance criteria prior to publicizing the meeting. In this regard, it is important to consider the false impression principle (see para 2–2).

c. Classified meetings.

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

(2) Approval for the disclosure of CMI to representatives of foreign governments and international organizations will be according to this regulation.

Section III
Nonacquisition-Related Meetings

G–6. Unclassified meetings

a. The conduct of cooperative development meetings involving only unclassified information does not require prior approval of ODCS, G–2; however, attendance by foreign representatives must be requested in the manner prescribed in appendix I of this regulation.

b. Coordination will be effected with all DA commands or agencies that may have a 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.

G–7. Classified meetings

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

b. Approval for the disclosure of CMI to representatives of foreign governments or international organizations will be according to this regulation.

Appendix H
Policy and Procedures for Disclosure of Classified Military Information in Support of International Activities

Section I
Introduction

H–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.

H–2. Policies and procedures on foreign involvement
The policies and procedures regarding foreign involvement in the materiel acquisition process are more complicated and warrant additional guidance (see apps B through E and app G).

Section II
Security assistance/direct commercial sale-related disclosures of classified military information

H–3. Policy
a. This section will cover 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, coproduction, 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 prospective 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 primarily involve the disclosure of information in categories 2, 4, and 8 (see para 2–4). In all cases where there is no 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, and so on) will be coordinated with OASA(ALT); ODCS, G–3; and ODCS, G–2 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 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. DA or DOD also may initiate this process unilaterally in anticipation of potential sales or transfers as a result of a foreign government's inquiry or a license application through the Department of State (required for DCS).

H–4. Disclosure of classified military information in security assistance initiatives
a. Disclosures pending decision of United States willingness to sell. Pending HQDA determination of its willingness to sell or otherwise transfer materiel to a specific foreign government or international organization, 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 information that is 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 price and availability (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 on countermeasures capabilities may not be considered for disclosure until the sale is consummated, and then only on a case-by-case basis. This information is deemed sufficient for a foreign government to make an informed judgement regarding potential acquisition or a purchase decision.

(2) After a foreign recipient has formally accepted an 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 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 noncooperative target recognition, and so on. 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 the DCS, G–2 or his or her designee and the NDPC.

H–5. Disclosure of classified military information on a licensed commercial basis

a. Mutual security assistance interests of the U.S. and foreign governments at times may be served better by the transfer of defense articles or services on a DCS basis. All commercial initiatives involving defense articles and services are subject to munitions licensing prescribed by the Department of State ITAR, which implements the Arms Export Control Act (AECA) (22 USC 2778–2780). OASA(ALT) 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 Army's munitions licensing review program. Overall DA policies and procedures governing the processing of munitions license applications are contained in AR 12–8.

(1) In coordination with OASA(ALT), DCS, G–2 or his or her designee 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. The FDO will also 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 for that weapon system, with assistance from the supporting FDO, will be responsible for overseeing the DCS cases involving his or her system 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 OASA(ALT); ODCS, G–3; ODCS, G–2; and USASAC.

b. Data regarding the status of the DA and DOD positions and substantive details regarding munitions license applications reviewed by DA and DOD are reflected in the SPAN.

H–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 (2), above, 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.

c. Proposals to authorize foreign test and evaluation in this manner will be submitted to OASA(ALT), which will—

(1) 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.

(2) Coordinate with the OASA(ALT); ODCS, G–2; and other HQDA staff agencies having an interest in the issue.

(3) On coordination and concurrence of all concerned, staff the issue with the Under Secretary of Defense for Acquisition and Technology.

(4) Provide to ODCS, G–2 a copy of the proposal. ODCS, G–2 will notify the NDPC Secretariat, as necessary.

d. The Secretary of the Army, in coordination with the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, approves the exception as satisfying the criteria in *b*(1) through *b*(3), above.

e. The test is performed pursuant to a test and evaluation agreement, lease arrangement, or sales contract containing requisite security controls.

f. Documentary CMI will be disclosed under this program only after both parties have approved the test program.

H–7. Disclosure of classified military information in security assistance-related training

Training of foreign representatives at DA activities or at U.S. contractor facilities under DA sponsorship will be conducted according to AR 12–1, AR 12–8, and AR 12–15.

a. DA CMI contained in training courses or otherwise to be presented to foreign trainees is 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 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 for 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 course material 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 foreign government or group of foreign governments.

d. DA agencies and commands conducting or supervising training may exercise discretionary authority to provide course-related classified documentary material (such as DA and school publications or student notes) to foreign trainees for their retention. 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 that third-country's government.

Section III
Research and Development (Materiel-Related Disclosure of Classified Military Information)

H–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 with 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 programs (AR 70–41).

(3) The Technical Cooperation Program (AR 70–41).

(4) Specific agreements covering one or more designated subjects (such as international participation in Army proponent programs covered by the Missile Defense Agency.

c. Excluded are agreements associated with the ESEP (AR 70–41) and MPEP (AR 614–10).

H–9. Disclosure in support of international cooperative research and development agreements

a. Proposed international cooperative R&D efforts involving the disclosure of CMI must be processed in accordance with AR 70–41, AR 550–51, and this regulation. Once approved, the associated DDL will govern the disclosure of CMI under the agreement. 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 an SSOI and DDL. The DDL will accompany the SSOI during the staffing process and be approved by the DCS, G–2 or his or her designee.

c. Except for codevelopment 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 Concept Technology Demonstration MOUs) will be considered on a

case-by-case basis. Such disclosures will require the concurrence of the DCS, G–2 or his or her designee, ASA(ALT), and the appropriate PM.

H–10. Classified military information 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 product improvement program (PIP)) will be according to the system TA/CP and DDL. Changes or improvements that, if incorporated, would significantly improve performance, decrease vulnerability to countermeasures, or otherwise constitute new classified information must be approved by the DCS, G–2 or his or her designee for disclosure prior to any commitment to international participation. For example, improvements that would require a new designation for an end item include the comparison of the AH–64A Apache and the AH–64D Apache (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.

H–11. Classified military information disclosure to foreign exchange and cooperative program personnel participating in Department of the Army research and development activities

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.

H–12. Foreign participation in classified acquisition contracts

For DA policy on foreign participation in classified acquisition contracts, see appendix G, section II.

Appendix I
Department of the Army International Visits Program

Section I
General

I–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.

I–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 respective governments 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 (such as badges and escorts) will apply for the control of foreign representative visitors in restricted access areas.

I–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 or designated foreign attaché staff personnel may propose and request visits by his or her country's officials. These proposals and requests become official only upon the submission of an RVA to ODCS, G–2 by appropriate foreign attaché personnel. While informal contacts with foreign representatives often may lead to the submission of an RVA, DA officials must remember that commitments made during these informal contacts are not binding for ODCS, G–2.

I–4. Classified military information documentary transfers

For detailed information on documentary requests for U.S. CMI, see paragraph 3–4.

I–5. Foreign Visits System requirements

An accredited military attaché or designee using the FVS will submit foreign government RVAs. Requests for visits by

governments that do not participate in the FVS will be submitted by the accredited military attaché, in writing, directly to ODCS, G–2, which will enter the request in the FVS and process it through the FVS.

I–6. Visit requests from countries without a military attaché

If a foreign government does not have a military attaché diplomatically accredited to the United States, 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 ODCS, G–2 for consideration. The RVA must conform to the policies and procedures for submission of RVAs in this regulation and DODD 5230.20.

I–7. Invitations

While foreign governments initiate the majority of foreign representative visits, DA officials also may initiate a foreign representative visit by extending a formal invitation.

a. Formal invitation. In instances when it is desirable to expend representational, security assistance, or International Military Education and Training (IMET) funds to invite foreign nationals or representatives (for example, speakers and participants in research projects) 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 published by competent authority. RVAs will not be used to effect these visits.

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 respective governments must defray all costs associated with the visit and an RVA must be submitted through the foreign government's embassy according to the self-invited visit procedures identified in section II of 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.

I–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 that person as a foreign representative.

I–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 ODCS, G–2 for action. See paragraph 1–4*f* for visits that are not governed by this regulation.

I–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

I–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 visit request, visitors or foreign military attaché personnel will contact the facility to be visited to arrange visit details.

b. Recurring visit authorizations. Recurring visit authorizations permit separate, one-time visits of fewer than 30 consecutive days over a specified period of time (normally 1 year) in connection with a government-approved license, contract, agreement, or other program. Authorizations will be valid for the duration of the program, subject to annual review, revalidation, and the specific requirements of the U.S. Army.

Note. By definition, any single visit of 30 consecutive days or more within the approved period of a recurring visit authorization constitutes an extended visit (see *c*, below) and therefore will require the submission of a separate request for extended visit authorization for this particular visit.

c. Extended visit authorizations. Extended visit authorizations (EVAs) will be used to permit a single visit for an extended period of time, normally 30 consecutive days or more. 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 PEP), or CPP to a DA activity.

(2) 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, approval by DCS, G–2 or his or her designee 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 start 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 the Military Attaché Guide issued by ODCS, G–2 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 ODCS, G–2 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 ODCS, G–2, which will provide instructions to the Army command or agency and notify the parent government's military attaché of the violation.

I–12. Assignment, evaluation, and processing of requests for visit authorization

a. Initial request for visit authorization review. Upon receipt in ODCS, G–2, the RVA will be screened to determine compliance with basic administrative requirements and will be either accepted for further processing 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) An 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) An 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 ODCS, G–2 is without prejudice; that is, staffing indicates only that DA has administratively accepted the RVA for processing and is not to be construed as either HQDA's solicitation of concurrence or as predisposition towards approval.

b. Request for visit authorization evaluation (administrative factors). In evaluating an RVA, the command or agency will apply the administrative factors listed 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 its 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. Request for visit authorization evaluation (substantive factors). In evaluating an 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, the organization should contact ODCS, G–3.

(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 either 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 should be disclosed to accomplish each aspect of the purpose of the visit and have 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 the DCS, G–2 or his or her designee. Such a proposal constitutes either a new disclosure program 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 B.

3. Army sponsorship of visits by foreign representatives to DA contractor facilities relieves the DA contractor from the licensing requirements of the ITAR and EAR. In these cases, the Army sponsoring command or agency assumes full responsibility for the visit, to include the provision of disclosure guidance to the DA contractor regarding the release of U.S. Army information. These visits will involve the disclosure of U.S. Army information in support of actual or planned international programs such as an FMS case and cooperative R&D arrangement. DA-sponsored visits will not be used to circumvent the licensing requirements of the ITAR.

d. Major Army command recommendation. The MACOM will recommend to ODCS, G–2—

(1) *Visits to DA command or agency.*

(a) Approval of the visit request and will 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 the POC, if not the same person; DDL number; international or functional agreement; advance coordination instructions for recurring RVAs; and so on).

(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, and so on).

(2) *Visits to DA contractor facility.*

(a) Approval of the visit request (this approval constitutes an Army-sponsored visit) and will 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 the POC, if not the same person; DDL number; international or functional agreement; advance coordination instructions for recurring RVAs; and so on).

(b) Not to sponsor the visit if it 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, denial, or nonsponsorship, the DCS, G–2 or his or her designee, on behalf of HQDA, will officially respond to the RVA.

(1) *Approval of request for visit authorization.* If the RVA is approved, notify the requester, affected Army elements, and DA contractors, as required, of the decision.

(a) Issue any instructions, limitations, and so on, 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 ODCS, G–2.

(2) *Denial or nonsponsorship of request for visit authorization.* If the RVA is denied or nonsponsored, notify the requester, affected Army elements, and DA contractors, as required, of the decision. Nonsponsorship of the RVA does not preclude the requester or the affected DA contractor from making direct arrangements according to ITAR provisions.

I–13. Letter of special accreditation

A letter of special accreditation is a document that is issued by the Director of Foreign Liaison, ODCS, G–2 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 specific DA commands or agencies without prior permission of HQDA (either the Director of Foreign Liaison, ODCS, G–2 or the Public Affairs Office). The Director of Foreign Liaison, ODCS, G–2 will provide copies of the Letters of Special Accreditation to the DA commands or agencies cited in the documents.

I–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 officials 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 appendixes J and K. 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 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. Contact officers for visiting foreign representatives will—

a. Become familiar with chapters 1 through 3 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. Make personnel with whom the visitors have official contact or exchange information 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 ODCS, G–2 through command channels.

Appendix J
Foreign Liaison Officers

J–1. Concept

The Army FLO program was established to facilitate cooperation and mutual understanding between the U.S. Army and the 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. The DCS, G–2 is the DA proponent for this program. 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 an LOA. Certification forms that are written specifically for a security assistance FLO (see sample at fig J–1) and DDLs are mandatory for these foreign representatives. See paragraph J–2*c*(3) for additional information.

Note. This category of FLOs also includes foreign representatives who are assigned to U.S. Army commands or activities under ITOs to perform specific administrative oversight functions regarding students of their respective governments. There will not be any disclosure of CMI to these FLOs. Certification forms and DDLs are not required 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.

Certification forms, as described in annex A to the country-specific liaison officer agreement between the U.S. Army and each foreign army participating in the FLO program, and a DDL are mandatory. For those countries that negotiated a liaison officer agreement without an annex for the certification form, use the generic certification form as shown in figure J–2. For the purposes of this regulation, a StanRep (see app K) is an operational FLO. A separate generic paragraph to describe the duties of an operational FLO that is also certified as a StanRep is shown in figure J–3, and will be placed in both the certification form and the DLL for these individuals. See paragraph J–2*c*(3) for additional information.

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. Certification forms and DDLs are not required for these foreign representatives. When a foreign national representative desires to visit a DA command or agency or a DA contractor facility on a frequent basis for a specific project, he or she may submit a one-time or recurring visit request to ODCS, G–2. In these cases, the foreign national representative will be acting as a FLO. All disclosure guidance will be the responsibility of the sponsoring Army command or agency.

J–2. Foreign liaison officer international agreement, letter of offer and acceptance and certification

a. International agreement. According to DODD 5230.20, when FLOs are physically assigned to U.S. Army installations in an operational capacity, an international 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 that is negotiated and concluded on behalf of DA by ODCS, G–2.

b. Letter of offer and acceptance. According to DODD 5230.20, when FLOs are physically assigned to U.S. Army installations in a security assistance capacity, an LOA is negotiated and concluded on behalf of DA by OASA(ALT) and contains provisions concerning such matters as responsibilities and obligations of the parties, authorized activities, security requirements (see fig J–4), financial arrangements, and claims.

c. Certification.

(1) *Purpose.* FLOs are assigned and 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 accomplishment 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 under which the FLO is assigned. Certification of a foreign representative as a FLO to more than one command or agency is not authorized.

(2) *Certification at a contractor facility.* DA certification may be used to sponsor the assignment of a FLO to a DA contractor facility. If DA chooses to certify a FLO to a DA contractor facility, the sponsoring DA command or agency will comply with the following conditions:

(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 CMI that is authorized for disclosure to that foreign government or international organization.

(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 and provided to DSS and the DA contractor, as required, for oversight purposes.

(3) *Certification statement form.* Each FLO is requested to sign a certification statement acknowledging the terms of his or her assignment. The contact officer is responsible for ensuring that the FLO understands and signs the certification statement form. A copy of the signed certification statement must be provided to the FLO. If a FLO declines 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 the ODCS, G–2.

J–3. Establishment of foreign liaison officer positions and processing of foreign liaison officer nominations

a. Establishment of foreign liaison officer positions. DA commands and agencies desiring to have FLOs assigned and certified 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 an international agreement or LOA. The procedures for establishing a new FLO position are as follows:

(1) *Request initiated by a foreign government for establishment of a foreign liaison officer position.*

(a) Step 1. A foreign government initiates a request for the establishment of a FLO position with the U.S. Army. DCS, G–2 or his or her designee 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.

(b) Step 2. The specified DA command or agency will evaluate the proposal and submit to ODCS, G–2 a recommendation to approve or disapprove the proposal. FLO position proposals must include 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. According to DODD 5230.20, a DDL is required for positions necessitating access to only unclassified information. The local commander may approve a DDL that only authorizes the disclosure of unclassified information. The local commander will provide a hardcopy version of the approved DDL to ODCS, G–2. (See app D.)

6. A clearly demonstrated 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. DCS, G–2 or his or her designee will coordinate the proposal within HQDA.

(d) Step 4. After HQDA coordination is completed, DCS, G–2 or his or her designee will finalize the decision on the proposal and formally notify the appropriate foreign government embassy. Upon notification of approval by the DCS, G–2 or his or her designee, the DA command or agency to which the FLO will be assigned will immediately begin to finalize the position DDL for approval. Upon receipt of the final draft DDL proposal, DCS, G–2 or his or her designee will review the document. Upon approval of the DDL, DCS, G–2 or his or her designee will notify the hosting Army command or agency and the appropriate foreign military attaché to proceed with the assignment of the FLO. 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 Department of the Army command or agency for establishment of a foreign liaison officer position.*

(a) Step 1. Prior to beginning discussions with foreign representatives on the establishment of a FLO position, DA commands or agencies must obtain the permission of the DCS, G–2 or his or her designee to proceed. Such proposals will be conveyed in writing through command or agency channels to ODCS, G–2.

(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. According to DODD 5230.20, a DDL is required for positions necessitating access to only unclassified information. The local commander may approve the DDL, with a copy furnished to ODCS, G–2. (See app D.)

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. DCS, G–2 or his or her designee will coordinate the proposal within HQDA.

(d) Step 4. After HQDA coordination is completed, DCS, G–2 or his or her designee 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, DCS, G–2 or his or her designee 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 DDL for approval. Upon receipt of the final draft DDL, DCS, G–2 or his or her designee will review the document. Upon approval of the DDL, DCS, G–2 or his or her designee 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 foreign liaison officer nominations. If the FLO position is established, DCS, G–2 or his or her designee will process the assignment of the FLO to a DA command or agency 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 ODCS, G–2 of the following:

(a) The FLO is an officially sponsored representative of that government.

(b) The FLO 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 establish acceptance of the FLO position.

(c) The FLO's legal status (including any privileges and immunities to which the individual is entitled).

(d) The FLO holds a specified level of security clearance.

(e) The FLO 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.* DCS, G–2 or his or her designee will process the EVA request to the DA command or agency to which the FLO is to be assigned. Since the position DDL outlining the terms of the certification of the FLO was precoordinated 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 either there is a significant change to the scope of the position or the position is terminated. See appendix D for detailed information on DDLs.

(3) *Step 3.* Upon receipt of the concurrence of the recipient DA command or agency, DCS, G–2 or his or her designee 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 will 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 ODCS, G–2, which 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 foreign liaison officer position. Any proposal to change the scope of a FLO's certification will be according to the procedures outlined in *a*, above, with emphasis on the specific modification. Any proposal to extend the FLO's assignment 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 the "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 foreign liaison officer 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 the DA continue to be served and that the purpose of the position remains valid. To facilitate the smooth transition of the incumbent and replacement FLOs, the host command or agency will commence a reevaluation of the position at least 90 days prior to the tour expiration date of the incumbent FLO to determine whether the host command or agency will recommend revalidation, modification, or termination of the FLO position. The host command or agency will notify ODCS, G–2 in writing of any recommendation to modify or terminate the FLO position.

J–4. 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 a dual capacity as a representative of their government and as a foreign exchange personnel participant (for example, a PEP, 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 nonrepresentational 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 the DCS, G–2 or his or her designee. Questions concerning the authorized activities of FLOs will be referred, through command or agency channels, to ODCS, G–2 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 J–4.

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 respective governments to assume responsibility as an agent of their respective governments and the approval of DCS, G–2 or his or her designee is granted. 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, or office nameplate) used by or issued to FLOs by the host Army command or agency will clearly identify the FLO as a foreign representative.

i. While assigned to a DA/DOD installation, 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 or DA contractor facility 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.

J–5. Administering foreign liaison officers

a. Visits.

(1) Visits by a FLO 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; these visits do not require official authorization from the DCS, G–2 or his or her designee.

(2) All visits by a FLO to destinations outside the terms of certification must be initiated by the parent government's military attaché through an RVA.

(3) All visits by a FLO 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 command or agency, a FLO may be granted supervised access to unclassified (to include CUI) sections of a command or agency library. 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. The provisions of AR 380–19 and local security procedures will apply.

d. Misconduct. When assigned to the U.S. Army, FLOs will conform to the Army's customs and traditions and will comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If a FLO violates the terms of certification; violates applicable law or DOD, DA, or local regulatory guidance; or otherwise conducts personal or professional affairs in an unsatisfactory manner, the hosting command or agency will provide a written report regarding the inappropriate action, through proper channels, to ODCS, G–2 with a recommendation for final disposition by HQDA, such as temporary suspension or permanent revocation of privileges, or revocation of certification. The DCS, G–2 or his or her designee will coordinate the resolution of all cases involving FLO misconduct.

J–6. Foreign disclosure officer

In support of this program, the FDO will be responsible for—

a. Assisting in the development of the DDL associated with each FLO position established within his or her command or agency.

b. Providing advice and assistance on all matters pertaining to the disclosure of CMI to each FLO assigned to the command or agency.

J–7. United States contact officer

a. Contact officers will be designated in writing by the commander, agency head, or a designee to facilitate and oversee the activities of FLOs at DA commands or agencies. The contact officer should be of equivalent rank/grade to the FLO (or higher, if available). 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.

b. The contact officer for a FLO will—

(1) Receive a briefing from the FDO and become familiar with this regulation and the specific terms of certification approved by the DCS, G–2 or his or her designee 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 certification statement form indicating his or her agreement and understanding of the duty assignment. The contact officer will provide a copy of the signed certification statement 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) Notify the ODCS, G–2 through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of FLOs under their oversight.

(6) Notify the supporting counterintelligence and local security offices of any foreign visitor activity that is reportable under the provisions of AR 381–12.

(7) Comply with the procedures cited in paragraph J–5*d* regarding misconduct on the part of the FLO.

(8) 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.

J–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, and so on) or to 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 the U.S. Army activity or installation is not necessary (that is, the FLO office is not located on the U.S. Army activity or installation). There are two types of foreign nationals that may be hired by FLOs as administrative support personnel: individuals in the United States on a work visa and 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 ODCS, G–2 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 an 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. An administrative support person that requires ingress and egress to restricted areas on an installation will be issued a foreign representative badge.

e. 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.

f. DDLs are not required for administrative support persons.

As a representative of (country) under the auspices the foreign military sales (FMS) case and an extended visit authorization to (place), I understand I am required to adhere to U.S. 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 in and of itself bestow diplomatic or other special privileges.

1. Responsibilities. I understand that my activities will be limited to the functions and responsibilities as outlined in the FMS case. 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 costs associated with my duties as a security assistance liaison officer will be allocated as outlined in accordance with the FMS case.

3. Extensions. I understand that if my government desires to request an extension 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 will be assigned to sponsor me during my visit to (place). I further understand that I will coordinate, through my contact officer, all requests for information, visits, and other business that fall under the terms of the FMS case.

5. Other Visits: I understand that visits to facilities for which the purpose does not directly relate to the terms of the FMS Case will be made through the Office of the Defense Attaché.

6. Uniform. I understand that I will wear my national uniform when conducting business at (place) unless otherwise directed or permitted. I will comply with the (name of country) 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 nonduty hours, I am required to notify my contact officer.

8. Security.

a. I understand that access to U.S. Government classified information will be limited to that information determined by my contact officer to be necessary to fulfill the functions of a security assistance liaison officer.

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 released or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the U.S. Government.

c. I will immediately report to my contact officer should I obtain or become knowledgeable of U.S. 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.

d. If required, I will display a security badge on my outer clothing so that it is clearly visible. The U.S. Government will supply this badge.

e. I understand that I may take custody of host government SECRET information to perform courier functions when authorized by the host participant.

f. I understand that all U.S. classified information is to remain under the control of the U.S. Army and is subject to U.S. security rules and regulations. 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 U.S. Army-supplied container and its contents will remain the responsibility of the U.S. Army, to include the security combination. Arrangements for the storage of (name of country) classified information must be accomplished in advance and in writing. The agreed procedures will require that the material arrives through government-to-government channels and that the U.S. Government provides receipts for the information.

g. I may not reproduce classified information for which I have assumed temporary custody. I am authorized to reproduce controlled unclassified information.

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.

Figure J–1. Sample of certification form for security assistance foreign liaison officers

I, (name of liaison officer), understand and acknowledge that I have been certified as a security assistance liaison officer to (place) as agreed upon by (name of country) and the U.S. Army. My contact officer and alternate contact officers are (name of contact officer and alternate contact officers).

(SIGNATURE OF SECURITY ASSISTANCE LIAISON OFFICER)
(TYPED NAME OF SECURITY ASSISTANCE LIAISON OFFICER)
(RANK AND/OR TITLE)
(DATE)
(SIGNATURE OF BRIEFER)
(TYPED NAME OF BRIEFER)

Figure J–1. Sample of certification form for security assistance foreign liaison officers—Continued

(Office symbol) (Date)

SECTION I
LIAISON OFFICER
LEGAL STATUS OF CERTIFICATION

As a representative of the (foreign government/international organization) under the auspices of an extended visit authorization to the U.S. Army, I am subject to the jurisdiction of U.S. Federal, State, and local laws, except as provided by treaty, other specific legal authority, or the terms of any diplomatic immunity that 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 in 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 will be assigned to sponsor me during my visit to the U.S. Army. I further understand that I will coordinate, through my contact officer, all requests for information, visits, and other business that fall under the terms of my certification. I also understand that requests for information that are beyond the terms of my certification will be made through the Office of the Defense Attaché.

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 U.S. 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 nonduty 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 U.S. escort officer to me during my nonduty access. Any cost incurred as a result of such nonduty access may be reimbursable to the U.S. 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 U.S. Army.

b. I understand that my administrative support person will not be permitted to act on my behalf or to 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.

Figure J–2. Sample of generic certification form for operational foreign liaison officers

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 U.S. 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.

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 by me to any other person, firm, organization, or government without the prior written authorization of the U.S. 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 U.S. 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 my contact officer should I obtain or become knowledgeable of U.S. 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 U.S. 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.

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, and so on. (Paragraph 5 of the DDL may be used as the basis to develop this section.)

3. Travel. I may visit the following locations under the terms of my certification, with the permission of my contact officer: (insert locations).

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

Figure J–2. Sample of generic certification form for operational foreign liaison officers—Continued

(DOD Service, agency or organization). I further acknowledge that I fully understand and have been briefed on the legal status of my certification, the conditions of my certification, and the terms of my certification. I further acknowledge that I will comply with the conditions and responsibilities of my certification.

(SIGNATURE OF SECURITY ASSISTANCE LIAISON OFFICER)
(TYPED NAME OF SECURITY ASSISTANCE LIAISON OFFICER)
(RANK AND/OR TITLE)
(DATE)
(SIGNATURE OF BRIEFER)
(TYPED NAME OF BRIEFER)

Figure J–2. Sample of generic certification form for operational foreign liaison officers—Continued

As a representative of (name of country) under the auspices of an extended visit authorization to (name of location), I understand I am required to adhere to U.S. Federal, State, and local laws, except as provided by treaty, other specific legal authority, or the terms of any diplomatic immunity that I may have been granted. I understand that my acceptance of the liaison officer position does not in and of itself bestow diplomatic or other special privileges.

CONDITIONS AND TERMS OF CERTIFICATION

1. Responsibilities. I understand that I am expected to present the views of my government with regard to the issues in 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 an operational liaison officer will be the responsibility of my government as outlined in the liaison officer Memorandum of Understanding/Agreement between the U.S. and (name of country) armies.

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 will be assigned to sponsor me during my visit to the U.S. Army. I further understand that I will coordinate, through my contact officer, all requests for information, visits, and other business that fall under the terms of certification. I also understand that requests for information that are beyond the terms of my certification will be made through the Office of the Defense Attaché.

5. Other Visits. I understand that authorization for visits to facilities for which the purpose does not directly relate to the terms of certification will be made through the Office of the Defense Attaché.

6. Uniform. I understand that I will wear my national uniform, where appropriate, when conducting business at the (Location of the U.S. facility) 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 nonduty hours, I am required to request assistance from my contact officer, who will provide the proper authorizations from the command security officer.

8. Security. I understand that—

a. 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 an operational 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 in accordance with 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 released or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the U.S. Government.

c. I will immediately report to my contact officer should I obtain or become knowledgeable of U.S. 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.

d. If required, I will display a security badge on my outer clothing so that it is clearly visible. The U.S. Government will supply this badge.

e. I may take custody of U.S. classified information to perform courier functions when authorized by the host participant certification for the liaison officer. I (am/am not) authorized to perform courier functions.

f. All U.S. classified material is to remain under the control of the host participant and is subject to inspection by host participant 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 participant-supplied container and its contents will remain the responsibility of the host participant, to include the security combination. Arrangements for the storage of parent participant classified information must be accomplished in advance

Figure J–3. Sample of certification form for specific operational foreign liaison officers

and in writing. The approved procedures will require that the material arrives through government-to-government channels and the foreign government provides receipts for the material.

g. I may not reproduce classified information for which I have assumed temporary custody. I am authorized to reproduce controlled unclassified information.

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.

10. Contact Officer and Alternate Contact Officer. (Insert name of contact officer and alternative contact officer) have been assigned as my contact officer and alternative contact officer.

11. Certification. I am certified to the U.S. Army in support of the following programs, topics, and so on:

a. Operational liaison duties.

b. Standardization representative duties. As an operational liaison officer certified to (name of location), I also have additional duties and responsibilities as a standardization representative under the auspice of the ABCA Standardization Program. When visiting U.S. Army installations to attend ABCA conferences or meeting or to conduct ABCA specific business at that site, I will not be required to have an embassy initiated visit request. Clearance certification and access to information will be provided directly from the parent ABCA organization to the meeting host, ODCS, G–3, ABCA program manager, or the Primary Standardization Office in Washington, DC. These clearances are not a function of the contact officer at (name of location).

12. Travel. I may visit the following locations under the terms of my certification with the permission of my contact officer: (insert names of locations).

I, (name of liaison officer), understand and acknowledge that I have been certified as a liaison officer to the U.S. Army (organization) as approved by the (name of country) Army and the U.S. Army. I further acknowledge that I fully understand and have been briefed on the legal status of my certification, the conditions of my certification, and the terms of my certification.

I further acknowledge that I will comply with the conditions and responsibilities of my certification.

(SIGNATURE OF SECURITY ASSISTANCE LIAISON OFFICER)
(TYPED NAME OF SECURITY ASSISTANCE LIAISON OFFICER)
(RANK AND/OR TITLE)
(DATE)
(SIGNATURE OF BRIEFER)
(TYPED NAME OF BRIEFER)

Figure J–3. Sample of certification form for specific operational foreign liaison officers—Continued

USASAC will ensure that the following standardized conditions and limitations are entered into the letter of offer and acceptance (LOA) for Foreign Liaison Officers.

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.

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 wearing 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 that 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.

Figure J–4. Foreign liaison officer letter of offer and acceptance conditions and limitations

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.

15. The Parent Party will ensure that the Liaison Officer complies at all times 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 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 Host Party, the Parent Government will remove the Liaison Officer or a family member 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 or her family member. 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 J–4. Foreign liaison officer letter of offer and acceptance conditions and limitations—Continued

Appendix K
Standardization Representatives

K–1. Concept

a. The ABCA Standardization Program began in 1947, when General Dwight D. Eisenhower and Field Marshal Bernard 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 Standardization Program has produced more than 1,000 standardization agreements, known as Quadripartite Standardization Agreements and Quadripartite Advisory Publications. The current ABCA Standardization Program is based upon the Basic Standardization Agreement (BSA) of 1964, which provides for the unencumbered exchange of information, equipment, and personnel between and among participating countries. The DCS, G–3 is the DA proponent for this program, and AR 34–1 is the proponent regulation.

Note. New Zealand personnel participate in the ABCA Standardization Program as observers with the Australian contingent.

b. Under the authority of the BSA, each of the armies participating in the ABCA Standardization Program exchange StanReps with each of the other armies in the program to conduct liaison between the "parent" army and the "host" army and to participate in ABCA activities in the "host" country. The British, Canadian, or Australian (BCA) StanReps in the U.S. are certified as operational FLOs, who perform the StanRep function as additional duties.

c. ABCA Quadripartite Working Groups (QWGs) are the basic forums used to exchange information and work on improving the capability of ABCA armies to operate together in a coalition environment. There are 13 QWGs and NPOCs represented in each group.

d. QWGs develop topics for inclusion on a standardization list (StanList), which is available online (http://www.abca.hqda.pentagon.mil). The army that is responsible for a particular topic on the StanList shares information regarding that topic with the other participating armies. Prior to inclusion on the StanList of any topic over which the U.S. Army will assume responsibility, the U.S. NPOC will ensure the normal foreign disclosure approval process as cited in this regulation is effected.

K–2. Standardization representative international agreement and certification

a. International agreement. The BSA of 1964 governs the assignment of StanReps to DA commands or agencies.

b. Certification. Certification will be according to the BSA of 1964 and paragraph J–2*c* of this regulation (see fig K–1).

K–3. Establishment of standardization representative positions and processing of standardization representative nominations

The procedures outlined in paragraph J–3 of this regulation apply for StanReps.

K–4. Conditions and limitations

The conditions and limitations outlined in paragraph J–4 of this regulation apply for StanReps.

K–5. Administering standardization representatives

The procedures outlined in paragraph J–5 of this regulation apply for StanReps. In addition, BCA StanReps are not required to coordinate with or seek the approval of their respective contact officer to attend any announced, formal ABCA meeting. They must coordinate all travel within the U.S. for nonformalized or non-ABCA meetings with their respective contact officer. Nonformalized or non-ABCA meetings are defined as those meetings not hosted by U.S. Army representatives or not approved by the ABCA Standardization Program.

K–6. Foreign disclosure officer

The responsibilities outlined in paragraph J–6 of this regulation apply. Additionally, in the event that a BCA StanRep requests U.S. Army information related to a specific topic on the StanList, the FDO should advise the StanRep to contact the parent government NPOC, who oversees the QWG for that particular topic. The list of the QWGs and associated NPOCs for each QWG is available online (http://www.abca.hqda.army.mil).

K–7. United States contact officer

The responsibilities outlined in paragraph J–7 of this regulation apply.

(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 U.S. Army, I am subject to the jurisdiction of U.S. Federal, State, and local laws, except as provided by treaty, other specific legal authority, or the terms of any diplomatic immunity that 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. Standardization Representative Duties. As a liaison officer certified to the (location of the U.S. Government facility), I also have additional duties and responsibilities as a standardization representative (StanRep) under the auspices of the ABCA Standardization Program. When visiting U.S. Army installations to attend ABCA conferences or meetings, I will not require an embassy-initiated visit request, but will provide my contact officer a copy of the official invitation. My government will provide my security clearance certification and other security assurance information to the conference or meeting host. In seeking information on a standardization list item, I understand that I am authorized to contact directly the custodian of that particular information. Furthermore, I understand that the contact information can be found on the ABCA Web site and any issues with these procedures should be addressed to my government's senior StanRep.

3. 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.

4. 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.

5. 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 U.S. Army. I further understand that I will coordinate, through my contact officer, all requests for information, visits, and other business that fall under the terms of my certification. I also understand that requests for information that are beyond the terms of my certification will be made through the Office of the Defense Attaché.

6. 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.

7. Uniform. I understand that I will wear my national uniform or appropriate civilian attire when conducting business at the (location of the U.S. Government facility) or other Department of Defense facilities, unless otherwise directed. I will comply with my parent government's service uniform regulations.

8. 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 nonduty 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 U.S. escort officer to me during my nonduty access. Any cost incurred as a result of such nonduty access may be reimbursable to the U.S. Government.

9. 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 U.S. Army.

Figure K–1. Sample certification statement

b. I understand that my administrative support person will not be permitted to act on my behalf or to 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 U.S. Immigration and Naturalization Service.

10. 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.

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 by me to any other person, firm, organization, or government without the prior written authorization of the U.S. Government.

c. I understand that all classified material (U.S. 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 U.S. 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 my contact officer should I obtain or become knowledgeable of U.S. 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 U.S. Government will supply this badge.

11. 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.

12. Terms not defined herein will have the definitions ascribed to them in the applicable agreement governing my assignment as a liaison officer.

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, and so on. (Paragraph 5 of the DDL may be used as the basis to develop this section.)

3. Travel. I may visit the following locations under the terms of my certification, with the permission of my contact officer: (insert names of locations).

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

Figure K–1. Sample certification statement—Continued

organization). I further acknowledge that I fully understand and have been briefed on the legal status of my certification, the conditions of my certification, and the terms of my certification. I further acknowledge that I will comply with the conditions and responsibilities of my certification.

(SIGNATURE OF SECURITY ASSISTANCE LIAISON OFFICER)
(TYPED NAME OF SECURITY ASSISTANCE LIAISON OFFICER)
(RANK AND/OR TITLE)
(DATE)
(SIGNATURE OF BRIEFER)
(TYPED NAME OF BRIEFER)

Figure K–1. Sample certification statement—Continued

Appendix L
Management Control Checklist and Department of the Army Staff Assistance and Compliance Visits

L–1. Function

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

L–2. Purpose

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

L–3. Instructions

The checklist below must be based on the actual testing of key management controls, such as document review, direct observations, and SPAN 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 five years. Commands and agencies shall use DA Form 11–2–R to certify the conduct of the evaluation.

L–4. Test questions

a. Has the FDO been appointed in writing? (See para 2–10*a*.) Has a copy been provided to the MACOM? (See para 2–10*a*.)

b. Does the FDO have copies of the required publications and documents? (See app A.)

(1) AR 380–5, Department of the Army Information Security Program.

(2) DODD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations.

(3) DODD 5230.20, Visits, Assignments, and Exchanges of Foreign Nationals.

c. Has the FDO attended the Army Foreign Disclosure Certification Course? (See para 2–10*b*.)

d. Have foreign representatives been properly certified to the command or agency? (See apps J and K.)

e. Have activities that foreign government officials have conducted that are outside of terms of certification been reported to the FDO and HQDA? (See paras J–4*b* and K–4.)

f. Does the contact officer maintain DDLs on all foreign representatives assigned to him or her? (See para D–4.)

g. Have contact officers been designated in writing to control the activities of foreign visitors? (See paras I–14, J–7*a*, and K–7.)

h. Have contact officers briefed the foreign representatives on DA and local policies affecting their status and performance of functions while assigned to DA organizations? (See paras J–7*b*(2) and K–7.)

i. Are DDLs prepared for each assigned foreign representative? (See paras J–1*a*, J–1*b*, and K–3.)

j. Are DDLs being maintained for all international programs requiring the disclosure of classified information? (See app D.)

k. Has the FDO disseminated approved DDLs to all concerned offices within and external to the command or agency, to include the contact officers? (See para D–4.)

l. Are disclosure decisions involving CMI based on a DDL? (See para 2–11.)

m. Are SPAN entries being made for CMI releases within 20 days of the actual first-time disclosure? (See para 3–7*b*.)

n. Did the command or agency obtain appropriate written authorization when disclosing U.S. CMI that is classified by another original classification authority? (See para 2–9.)

o. Is the FDO reviewing munitions license applications to ensure policy compliance, particularly when the license application involves the export of U.S. classified information? (See para H–5.)

p. Do SPAN RVA approval recommendations include, at a minimum: the name and duty phone number of the contact officer and/or POC, DDL number, international or functional agreement, and advance coordination instructions for recurring visits? If denial is recommended, is rationale provided? (See para I–12*d*.)

q. Are recurring RVAs approved only in support of approved licenses, contracts, or other government programs? (See para I–11.)

r. Are visit requests to contractor facilities reviewed to ensure that visits not in support of an actual or an approved, planned DA program are denied? (See para I–12.)

s. Did contact officers receive guidance from the FDO regarding visits that will involve the disclosure of U.S. CMI? (See para I–14.)

t. Did the contact officer discuss responsibilities and duties of the foreign representative's assignment during initial in-brief and provide a copy of the job description and signed certification form to the foreign representative? (See paras J–7*b*(2) and K–7.)

u. Is foreign disclosure included in the installation security program? (See paras 1–4*a*(2), 1–4*a*(3), 1–4*b*, 1–4*f*, and 3–2.) (In accordance with AR 190–13 for physical security and AR 380–5 for information security.)

L–5. Supersession

This checklist replaces the checklist previously published in AR 380–10, dated 15 February 2001.

L–6. Comments

Help make this a better tool for evaluating management controls. Submit comments to the Office of the Deputy Chief of Staff, G–2, ATTN: DAMI–CDD, 1000 Army Pentagon, Washington, DC 20310–1000.

Glossary

Section I
Abbreviations

ABCA
American, British, Canadian, and Australian Armies

AECA
Arms Export Control Act

AMC
U.S. Army Materiel Command

APD
U.S. Army Publishing Directorate

AR
Army regulation

ASA(ALT)
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

ATPO
associate technical project officer

BCA
British, Canadian, and Australian

BSA
Basic Standardization Agreement

CG
commanding general

CIA
Central Intelligence Agency

CIO/G–6
Chief Information Officer/G–6

CMI
classified military information

COE
Chief of Engineers

COMSEC
communications security

CONUS
continental United States

CPI
critical program information

CPP
cooperative program personnel

CSA
Chief of Staff, U.S. Army

CUI
controlled unclassified information

DA
Department of the Army

DCI
Director, Central Intelligence

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3
Deputy Chief of Staff, G–3

DDL
delegation of disclosure authority letter

DEA
data exchange annex

DIA
Defense Intelligence Agency

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DSS
Defense Security Service

DTIC
Defense Technical Information Center

DUSA(OR)
Deputy Under Secretary of the Army (Operations Research)

EAR
Export Administration Regulations

ECP
engineering change proposal

ENDP
exception to the National Disclosure Policy

ESEP
Engineers and Scientists Exchange Program

EVA
extended visit authorization

FDO
foreign disclosure officer

FDS
foreign disclosure system

FLO
foreign liaison officer

FMS
foreign military sales

FOIA
Freedom of Information Act

FORSCOM
U.S. Army Forces Command

FVS
Foreign Visits System

GPO
Government Printing Office

GSOMIA
General Security of Military Information Agreement

HQDA
Headquarters, Department of the Army

IEA
information exchange annex

IMET
International Military Education and Training

INSCOM
U.S. Army Intelligence and Security Command

ITAR
International Traffic in Arms Regulations

ITO
invitational travel orders

JCS
Joint Chiefs of Staff

LOA
letter of offer and acceptance

MACOM
major Army command

MCTL
Militarily Critical Technologies List

MOU
Memorandum of Understanding

MPEP
military personnel exchange program

MSC
major subordinate command

MWO
modification work order

NATO
North Atlantic Treaty Organization

NDP
National Disclosure Policy

NDP–1
National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations, short title: National Disclosure Policy (NDP–1)

NDPC
National Disclosure Policy Committee

NIPRNET
Non-Secure Internet Protocol Router Network

NISPOM
National Industrial Security Program Operating Manual

NORAD
North American Air Defense Command

NPOC
national point of contact

NTIS
National Technical Information Service

OASA(ALT)
Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

OCONUS
outside the continental United States

ODCS, G–2
Office of the Deputy Chief of Staff, G–2

ODCS, G–3
Office of the Deputy Chief of Staff, G–3

OPSEC
operations security

OSD
Office of the Secretary of Defense

P&A
price and availability

PEO
program executive office

PEP
U.S. Army Personnel Exchange Program

PIP
product improvement proposal

PM
program manager

POC
point of contact

PPP
program protection plan

QWG
Quadripartite Working Group

RA
record of action

R&D
research and development

RFI
request for information

RFP
request for proposal

RSI
rationalization/standardization/interoperability

RVA
request for visit authorization

SCI
sensitive compartmented information

SCG
security classification guide

SIPRNET
Secret Internet Protocol Router Network

SMDC
Space and Missile Defense Command

SPAN
Security Policy Automation Network

SSOI
summary statement of intent

StanList
standardization list

StanRep
standardization representative

TA/CP
technology assessment/control plan

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

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, U.S. Army

Section II
Terms

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 presolicitation proposal, prebidder, and preaward 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 or field-operating mission. A unit or organization that 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
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—research, development, test, and evaluation
Descriptions of budget activities 1–3 are provided below.

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 subsequent exploratory and advanced developments in defense-related technologies as well as for 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.

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 nonsystem-specific development efforts. The 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 normally will be exercised by a general level of effort. Exploratory development precedes the system-specific research.

Budget activity 3 (BA3)—advanced development
Includes all efforts that have moved into the development and integration of hardware and other technology products for field experiments and tests. 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 transitions from the laboratory to operational use. Projects in this category have a direct relevance to identified military needs. Advanced development may include concept exploration, 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 (TOP SECRET, SECRET, or CONFIDENTIAL) by the contractor or its employees in the performance of the contract. The contract may be a classified contract even though the contract document is not classified.

Classified military information
Information originated by or for the DOD or its agencies or under their jurisdiction or control that requires protection in the interest of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL as described in Executive Order 12958 or subsequent order. Classified military information may be in oral, visual, documentary, or materiel form.

Combined information
Military information that, by agreement, is declared to be combined by the USG 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
Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the USG. It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.7, AR 25–55, AR 340–21, AR 530–1, and so on, or that is subject to export controls according to the ITAR or the EAR.

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 PM (or PM 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.

Coproduction
Method by which items intended for military application are produced under the provisions of a formal agreement that provides for the transfer of technical information and know-how from one government to another.

Critical Program Information
Critical program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

Critical technology
Technology that consists of arrays of design and manufacturing know-how (including technical data); keystone manufacturing, inspection, and test equipment; keystone materials; and goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country—or combination of countries—and compromise of which may prove detrimental to U.S. security.

Data exchange annex
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
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 HQDA or by DA's principal disclosure authority to control disclosures of classified military information by his or her organization to foreign governments and 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
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.

Executive agent
The DA office or organization that has overall responsibility and oversight for a program.

Export Administration Regulation
Governs exports of dual-use items. It also provides discussions of certain key regulatory policy areas, including policies governing exports of high-performance computers, exports of encryption products, deemed exports, U.S. antiboycott regulations, special regional considerations, the multilateral export control regimes, and the technical advisory committees.

Extended visit authorization
See visit authorization.

Foreign disclosure officer
DA member designated in writing to oversee and control coordination of specific disclosures of CMI. FDOs are authorized for appointment to lowest command level that is the proponent for Army-created, developed, or derived CMI.

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
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. There are three types of FLOs. A security assistance FLO is a foreign government representative who is assigned to a DA element or contractor facility pursuant to a requirement that is described in an FMS LOA. An operational FLO is a foreign government representative who is assigned to a 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. A national representative FLO is a foreign government representative who is assigned to his or her national embassy or legation in Washington, DC (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 United States 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 representative
For the purposes of this regulation, foreign nationals or U.S. citizens or nationals who are acting as representatives of either a foreign government or a 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
Automated system operated by the Office of the Under Secretary of Defense (Policy) that provides staffing and database support for processing requests for visits by foreign nationals to DOD activities and defense contractors. FVS consists of an unclassified segment that allows the online submission of visit requests from embassies in Washington, DC, and, in some cases, directly from foreign governments overseas. FVS also has a classified segment that provides staffing, decisionmaking support, and database capabilities to the military departments and DIA.

Functional agreement
An agreement not formally deemed to be an international agreement, including contracts made under the Federal Acquisition Regulations; FMS credit agreements; FMS LOAs or defense sales agreements; FMS letters of intent; 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; leases under 10 USC 2667 or 2675; leases under 22 USC 2796; and agreements that establish only administrative procedures.

Government-to-government channels
Principal 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.

Hosted visit
A visit by official nationals of a foreign government under the auspices of an invitation that is extended by a DA official.

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 the auspices of both 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 codevelopment, dual production, DDEPs, and security assistance programs.

International agreement
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 is signed or agreed to by civilian or military officers, employees of any DOD organizational element, or representatives of the Department of State or other agencies of the USG; signifies the intention of the parties to be bound in international law; and is identified as an international agreement, MOU, 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.

Any oral agreement that meets the preceding criteria. Such an agreement must be reduced to writing by the DOD representative who enters into the agreement.

A NATO Standardization Agreement that provides for either mutual support or cross-servicing of military equipment, ammunition, supplies, and stores or mutual rendering of defense services, including training.

International organization
Entity established by recognized governments pursuant to international agreement that, 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
Department of State implementation of Section 38 of the AECA (22 USC 2778–2780). ITAR governs export of information and materiel that are defense-related and listed on the U.S. Munitions List.

International Visits Program
The program that is established to process visits by and assignments of foreign representatives 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 DOD components, or two or more Federal departments or agencies, exercise control, jurisdiction, or security awareness.

Letter of offer and acceptance
U.S. document by which the USG offers to sell to a foreign government or international organization defense articles and defense services pursuant to the AECA, as amended. The LOA lists the items and/or services, estimated costs, and terms and conditions of sale and provides for the foreign government's signature to indicate acceptance.

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 (ODCS, G–2 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 the 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.)

Munitions license
A document bearing the word *license*, issued by the Director, Office of Defense Trade Controls or his or her authorized designee, that 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 subject to licensing requirements imposed by AECA through the 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
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. General members will serve as representatives of the Secretaries of State, Defense, Army, Navy, and Air Force and the Chairman, Joint Chiefs of Staff. 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, Technology and Logistics; Assistant Secretary of Defense for Command, Control, Communications and Intelligence; Assistant to Secretary of Defense (Atomic Energy); Director, Defense Intelligence Agency; and Director, Missile Defense Agency.

One-time visit authorization
See visit authorization

Original 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.

Original classification
An initial determination that, in the interest of national security, information requires protection against unauthorized disclosure.

Personnel Exchange Program
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.

Proponent
Army organization or staff element that has primary responsibility for materiel or subject matter expertise in its area of interest or is charged with accomplishment of one or more functions.

Proprietary information
Classified or unclassified proprietary information, the rights to which are owned by private firms or citizens (for example, patents, copyrights, or trade secrets). Disclosure cannot be effected without the owner's consent unless such disclosure is authorized by relevant legislation, and then release will be subject to such legislation.

Rationalization/standardization/interoperability
Means of increasing coalition warfare capabilities of U.S., 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 nonmateriel requirements and is essential to successful integration of allied forces during conduct of combined operations.

Record of action
Official record of NDPC decisions on ENDP requests.

Recurring visit authorization
See visit authorization

Security assistance
Group of programs authorized by the Foreign Assistance Act of 1961, as amended, and AECA, 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 Policy Automation Network
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
In the context of a meeting, provision of DA resources (such as personnel and funds) in support of the meeting.

In the context of a visit by a foreign visitor to U.S. industry, DA authorization for disclosure of information on U.S. 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).

In the context of a visit by a 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
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 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
Any blueprint, drawing, plan, instruction, computer software and documentation, or other technical information that can be used or 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 program
International TRDPs 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 U.S. and second country or international organization.

Third party transfer
Transfer of U.S. defense articles, services, and training to 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 representatives in the United States or overseas either by officers or employees of the United States, contract technicians, or contractors (including instruction at civilian institutions) or through 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.

According to 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.

According to 8 USC 1324b(a)(30), the term *protected individual* means an individual who is a citizen or national of the United States or is an alien who is lawfully admitted for permanent residence, is granted the status of an alien lawfully admitted for temporary residence under 8 USC 1160(a) or 8 USC 1255a(a)(1), is admitted as a refugee under 8 USC 1157, or is granted asylum under 8 USC 1158. The term does not include an alien who fails to apply for naturalization within 6 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 6 months after November 6, 1986. The term also does not include 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 *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. 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. 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 for more than 30 days for one of the following situations: 1) certification as a FLO, foreign exchange personnel (ESEP or PEP), 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 Army's interest, Army-sponsored training at a contractor or Army facility under DCS); or 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

This index is ordered alphabetically by topic and subtopic. Topics and subtopics are identified by paragraph number.

Army Materiel Command (AMC)
Responsibilities, 1–12
TCP, 4–2
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
Delegated disclosure authority, 2–8*b*(1)(b), 2–8*b*(1)(c)
Responsibilities, 1–7
TCP, 4–2

Channels of official foreign disclosure communications, 1–4*a*(2)
Chief of Engineers
Responsibilities, 1–10
Chief Information Officer/G–6
Delegated disclosure authority, 2–8*b*(1)(a), 2–8*b*(1)(b), 2–8*b*(1)(c)
Responsibilities, 1–10
TCP, 4–2
Classified military information
Definition, 2–3*a*
DTIC document requests, 3–4*c*
NDP–1 categories, 2–4
Procedures for requesting documents, 3–4*d*, 3–4
Requests for documents, 3–4
Requests for security assistance documents, 3–4*a*
Requests for R&D documents, 3–4*b*
Requests for other documents, 3–4*d*
Transmittal of documents to foreign governments, 3–6
Computers and computer networks, 3–8, J–5*c*
Conferences (meetings and symposia)
Acquisition–related, G–3 through G–5
Approval policies, G–1
Nonacquisition–related, G–7, G–6
Rationalization/standardization/interoperability (RSI)–related, G–3
Contact officer
Responsibilities, foreign liaison officer (FLO), J–7
Responsibilities, foreign visit, I–14
Responsibilities, standardization representative (StanRep), K–7
Contacts with foreign representatives, 1–4*a*(3)
Controlled unclassified information, 1–4*e*(10), 2–3*b*(1)

Delegated disclosure authority
Emergency authority, 2–8*b*(5)
HQDA disclosure authorities, 2–8*b*
Redelegation, 2–8*b*(4)
Delegation of disclosure authority letter (DDL)
Format, D–5
General, 2–8*b*(3), 2–8*b*(4), 2–8*a*, 2–9, 2–11*a*, 4–3*c*, 4–3*b*, D–1
Position DDL, D–3
Preparation, D–4
Requirement, D–2
Deputy Chief of Staff, F–2
Delegated disclosure authority, 2–8
Responsibilities, 1–5
Role in disclosure, 2–11*a*
TCP, 4–2
Deputy Chief of Staff, F–3
Delegated disclosure authority, 2–8*b*(1)(a) through 2–8*b*(1)(c), 2–8*b*(1)(e), 2–8*b*(1)(f)

Responsibilities, 1–8
Deputy Under Secretary of the Army for Operations Research, 1–6

Eighth U.S. Army, 1–15
Exception to the National Disclosure Policy (ENDP), See also National Disclosure Policy
Format, B–2
Requests, 2–5*c*, B–1

False impression, 2–2
Foreign access to computers, 3–8, J–5*c*
Foreign disclosure channels and general decision procedures, 2–11
Foreign disclosure officer (FDO)
Appointment, 2–10*a*
Definition and responsibilities, 2–10
Roles, J–6, K–6
Training, 2–10*b*
Foreign liaison officer (FLO)
Administering, J–5
Administrative support personnel, J–8
Certification, J–2*c*
Conditions and limitations, J–4
Contact officer responsibilities, J–7
Establishment, J–3*a*
FDO responsibilities, J–6
National representative, J–1*c*
Operational FLO, J–1*b*
Sample certification statement, J–1*a*, J–1*b*
Security assistance FLO, J–1*a*
Foreign test and evaluation, H–6
Frequently asked questions, F–2, F–1

HQDA agency heads, 1–11

Information not governed by this regulation, 1–4*e*
International Visits Program
Concept, I–1
Contact officer responsibilities, I–14
Extended visit request, I–11*c*
Funding, I–10
Informal coordination, I–3
Invitations, I–7
Letter of special accreditation, I–13
One–time visit request, I–11*a*
Out–of–channel request, I–9
Processing visit request, I–12
Recurring visit request, I–11*b*
Standards of appearance, I–8

Major Army commands (MACOMs), 1–11
Management Control Evaluation Checklist, L–1 through L–4
Meetings. See Conferences
Military information
Categorization, 2–3
NDP Categories 1 through 8, 2–4*b*(1) through 2–4*b*(8)

National Disclosure Policy Committee, 1–5*c*, 2–5*c*, 2–8*b*(1)(d), B–1*c*, H–4*d*(2)
National Disclosure Policy (NDP–1), 1–5*b*
Categories of CMI, 2–4
Disclosure levels, 2–5*a*, 2–5
Exceptions to NDP–1 (ENDPs), 2–5*c*, B–2, B–1

National Defense Strategy, 2–1

OCONUS Army activities (non–MACOMs), 1–16
OCONUS MACOMs, 1–15
Official communications with foreign representatives
Channels, 1–4*a*(3)

Policy, 1–4
Program protection plan (PPP), 4–3*a*
Public domain information, 2–3*b*(2)

Redelegation of disclosure authority, 2–8*b*(4), D–5

Security Policy Automation Network (SPAN), 2–8*b*(2), 3–4*c*(5), 3–7, H–5*b*, L–4*m*, L–4*p*
Security protection and assurances, 2–6*a*(2)
Standardization representative (StanRep)
Administering, K–5
Certification, K–2*b*
Concept, K–1
Conditions and limitations, K–4
Contact officer responsibilities, K–7
Establishment, K–3
FDO responsibilities, K–6
Sample certification statement, K–2*b*
Summary statement of intent (SSOI)
Background, 4–3*c*, E–1
Format, E–2

Technology assessment/control plan (TA/CP)
Background, 4–3*b*
Development, C–2
Format, C–2
Technology control panel, 4–2
The Judge Advocate General
Responsibilities, 1–9
TCP, 4–2
The Surgeon General
Delegated disclosure authority, 2–8*b*(1)(a), 2–8*b*(1)(b), 2–8*b*(1)(e)
Responsibilities, 1–10
TCP, 4–2

U.S. Army Criminal Investigation Command
Responsibilities, 1–14
U.S. Army Europe, 1–15
U.S. Army Intelligence and Security Command
Responsibilities, 1–13
U.S. Army Pacific, 1–15
U.S. Army Southern Command, 1–15
United States/Canada Joint Certification Program, 1–4*f*(10)

Visits not governed by this regulation, 1–4*f*

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 202

PIN:	004070–000
DATE:	06- 3-03
TIME:	08:10:28
PAGES SET:	91
DATA FILE:	C:\wincomp\r380-10.fil
DOCUMENT:	AR 380–10
SECURITY:	UNCLASSIFIED
DOC STATUS:	REVISION