Army Regulation 380–10

Security

Foreign Disclosure and Contacts with Foreign Representatives

Headquarters
Department of the Army
Washington, DC
4 December 2013

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

This major revision, dated 4 December 2013--

- Assigns Headquarters, Department of the Army the responsibility of developing and coordinating community-wide foreign disclosure training and education requirements (para 1-6*r*).

- Adds responsibilities for the Deputy Chief of Staff, G-4, Deputy Chief of Staff, G-8, the Chief, National Guard Bureau, and the Chief, Army Reserve (paras 1-9, 1-10, and 1-14).

- Expands the five-year delegation of disclosure authority letter expiration rule to all delegation of disclosure authority letters (para 2-10).

- Clarifies language regarding who may approve delegation of disclosure authority letters that only authorize the disclosure of controlled unclassified information (para 2-10*b*).

- Introduces the concept of the foreign disclosure representative and outlines the foreign disclosure representative's duties and responsibilities (para 2-11*b*).

- Establishes general policy for foreign disclosure education programs (para 2-12).

- Introduces SENTRY as the Army's official foreign disclosure repository and disclosure decision support system (para 4-1).

- Requires that requests for visit authorizations be submitted on all foreign representatives who are travelling on invitational travel orders with the exception of foreign government personnel who are travelling for training purposes (para I-7*a*).

- Reinstates foreign disclosure guidance and/or considerations for Military Personnel Exchange Program Personnel, Engineer and Scientist Exchange Program Personnel, and Cooperative Program Personnel (apps L through N).

- Outlines the responsibilities of the contact officer (app O).

- Prescribes the duties and responsibilities of the visit point of contact (para O-7).

- Provides policy and procedures for the disclosure of controlled unclassified information (throughout).

Headquarters
Department of the Army
Washington, DC
4 December 2013

*Army Regulation 380–10

Effective 4 January 2014

Security

Foreign Disclosure and Contacts with Foreign Representatives

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation provides policy and procedures for the disclosure of Army classified military information and controlled unclassified information to foreign governments and international organizations; policy regarding contacts with foreign representatives; policy and procedures for the Department of the Army International Visits Program; certification of foreign liaison officers to Department of the Army commands, installations, and contractor facilities for which the Department of the Army is the lead agent or has security cognizance; guidelines for foreign representative attendance at Army-sponsored meetings, conferences, and symposia; and establishment of policy, procedures, and assignment of responsibilities for 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), DODDs 5230.11, and 5230.20.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve. It applies to all personnel involved in the foreign disclosure and technology 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 or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix P).

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 (DAMI–CDD), 1000 Army Pentagon, Washington, DC 20310–1000.

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 Deputy Chief of Staff, G–2 (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/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 380–10, dated 22 June 2005.

UNCLASSIFIED

Contents—Continued

Contents—Continued

Contents—Continued

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) and relevant controlled unclassified information (CUI), as specified in paragraph 1–5*a*(2), to foreign governments and international organizations; contacts with foreign government representatives; certification of foreign liaison officers to Department of the Army (DA) commands, installations, and contractor facilities for which DA is the lead agent or has security cognizance; and foreign government representative attendance at Army-sponsored meetings, conferences, and symposia. 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. Responsibilities
Responsibilities are listed in section II of chapter 1.

1–5. Authority
a. This regulation prescribes DA policies and procedures governing the disclosure of CMI and certain CUI to foreign governments and international organizations and contacts with foreign government representatives.

(1) *Disclosure of classified military information.* This regulation governs the disclosure of CMI 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 (EO) 13526. CMI may be in oral, visual, or documentary form (see Army regulation (AR) 380–5).

(2) *Disclosure of controlled unclassified information* This regulation also governs the foreign disclosure of CUI identified in DODM 5200.01 which applies to all unclassified information (including doctrinal and training information) with military or space applications that does not meet the standards for national security classification under EO 13526, but is pertinent to the national interests of the U.S. and is in the possession of, or under the control of, a DOD component.

Note. Not all CUI is marked or has a distribution statement. It is incumbent upon all originators and proponents to review material prior to making a disclosure determination, in order to appropriately identify the information as public domain or CUI.

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

(a) On behalf of the Secretary of the Army and the Chief of Staff, Army (CSA), the Deputy Chief of Staff, G–2 (DCS, G–2) or their 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. For the purposes of this regulation, the term "foreign military attaché" applies to both the principal accredited military attachés and accredited assistant military attachés. In addition, the DCS, G–2 is the Army lead agent for all official foreign government requests for visits to DA commands or activities and for Army information. All official foreign contacts with the Army in the continental United States (CONUS) must be requested by military attachés diplomatically accredited to the Army 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 their 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 the Deputy Chief of Staff, G–2 (DCS, G–2) of such unauthorized contact is necessary.

(c) All foreign national requests for information from, and/or contact with, DA personnel or DA organizations, regardless of the mode of transmittal (such as correspondence and email), must be referred to the supporting public

affairs office for appropriate action. Except as required by AR 381–12, no report to DCS, G–2 of such unauthorized contact is necessary.

(4) *Contacts with foreign representatives*. This regulation governs activities and actions involving representatives of foreign governments and international organizations. Inherent in all contacts with foreign representatives is the exchange of information in various forms—oral, visual, or documentary. Policies governing the disclosure of DOD and DA information outside the USG prescribe that disclosed information must be suitable for disclosure to the public or to foreign governments or international organizations in furtherance of a legitimate USG purpose. Therefore, 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 and 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 their government to act as an official representative of that government in its dealings with the Army in connection with programs, projects, or agreements of mutual interest to the Army and the foreign government.

(c) Foreign personnel exchange programs (PEP). Military or civilian officials of a foreign defense establishment who are assigned to a U.S. DOD component (such as the Army) according to the terms of an applicable international agreement and who perform duties prescribed by a position description for the DOD component (see 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 (see AR 70–41).

(e) Meetings and symposia. Attendance by foreign representatives at meetings 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 and CUI to foreign representatives.

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

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

c. This regulation prescribes the duties and responsibilities of personnel designated as foreign disclosure officers (FDOs) and foreign disclosure representatives (FDRs).

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

e. This regulation prescribes the duties and responsibilities of personnel designated as visit POCs for foreign representatives who are visiting DA commands or agencies.

f. 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 (see AR 380–28).

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

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

(4) *Nuclear information*. Nuclear-related information (restricted data or formerly restricted data) (see 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 (see 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 (see AR 380–5).

(8) *Automated information systems information outside the continental United States*. Unclassified information that

has been, is, or can be deemed suitable for disclosure to local nationals employed in overseas Army computer and/or communications facilities (see AR 25–2).

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

(10) *Controlled unclassified information*. Controlled unclassified information not covered under paragraph 1–5*a*(2) to which access or distribution limitations have been applied according to national laws, policies, and regulations of the USG. These types of information include but are not limited to: patent secrecy data, confidential medical records, inter- and intra-agency memoranda that are deliberative in nature, certain data compiled 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 CUI under 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, when such release is to U.S. permanent resident aliens*. U.S. permanent resident aliens' access to CMI is governed by AR 380–5.

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

(13) *Information in the public domain*. Unclassified information that has been, is, or can be deemed suitable for disclosure to the public at large (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) *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 disclosure will be subject to such legislation.

g. The visit request requirements of this regulation do not apply to the following:

(1) Non-government-to-government visits (see 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, international military students, or private individuals attending school at educational facilities under contract with the Army or any other governmental component (see AR 12–15).

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

(4) Cross-border movements of U.S. and Canadian forces (see 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 (see DOD 5220.22–M).

(6) Visits to Army or DA contractor facilities by foreign national employees of U.S. contractors (see DOD 5220. 22–M).

(7) Visits by foreign representatives or foreign nationals sponsored by another DOD or Federal agency (see AR 190–13). For example, a foreign delegation sponsored by the Office of the Secretary of Defense (OSD) that will be visiting an Army installation under OSD supervision does not require a visit request. OSD must conduct pre-coordination with the installation and/or command to be visited.

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

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

(10) Visits for activities that are open to the public or hosted by the public affairs office (see 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.

(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 (see 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 (see AR 190–13).

h. This regulation specifically prohibits the disclosure of classified or controlled unclassified:

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

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

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

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

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

i. This regulation does not affect or modify the responsibility vested in the Director of National Intelligence 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 Director of Central Intelligence 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.

Section II
Responsibilities

1–6. 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 for technology protection (that is, counterintelligence, intelligence, security, and foreign disclosure) support to the Technology Transfer Program. The internal control evaluation checklist is provided at appendix P.

b. Administer, manage, and execute the Army's International Visits Program as defined by this regulation. The DCS, G–2 may delegate to specific DA elements the authority to approve certain types of visits by foreign representatives.

c. Develop and oversee the implementation of Army policies governing contact with, and disclosure of CMI, to foreign representatives and provide general guidance, advice, and assistance to DA officials determining the suitability of CMI and relevant CUI 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), Department of Defense Directive (DODD) 5230.11, DODD 5230.20, DODD 5530.3, and Department of Defense Instruction (DODI) 2040.02. The DCS, G–2 will—

(1) Exercise sole approval authority for disclosure of DA CMI to foreign governments as well as authority to delegate CMI disclosure authorizations to Army commands (ACOMs), Army service component commands (ASCCs), direct reporting units (DRUs), and DA elements.

(2) Exercise oversight of CUI disclosure authorizations issued by ACOMs, ASCCs, DRUs, and DA elements.

d. Provide foreign disclosure advice and guidance to the DA staff.

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

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

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

h. Be the primary POC for technology protection issues within Headquarters, Department of the Army (HQDA).

i. Ensure all first-time disclosure decisions involving CMI are recorded in the Security Policy Automation Network (SPAN) in compliance with this regulation and DODD 5230.11.

j. Record decisions on foreign government requests for visit authorization to DA elements in the Foreign Visits System (FVS) in compliance with this regulation and DODD 5230.20.

k. Administer, manage, and execute the Foreign liaison Officer (FLO) Program.

l. Conduct oversight of the FLO Program.

m. Exercise exclusive authority over the approval of all Army delegation of disclosure authority letters (DDLs).

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

o. 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.

p. Coordinate all foreign government requests for information (RFIs).

q. Conduct periodic on-site visits to ACOMs, ASCCs, and DRUs to ensure compliance with this regulation.

r. Develop and coordinate community-wide training and education requirements and best business practices as part of service-level governance and oversight.

s. Conduct a periodic (at least biennially) foreign disclosure conference.

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

The ASA (ALT) will—

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

b. Appoint, in writing, a DA member to be the FDO, and FDRs as appropriate.

c. 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).

d. 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).

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

f. Provide a review and recommendation for the Committee on Foreign Investment in the U.S. determination regarding CMI and/or CUI disclosure as a result of foreign investment and provide an assessment of the associated risk.

g. Manage and oversee International Cooperative Armament Agreements and the Foreign Comparative Testing Program.

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

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

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

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

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

n. Manage the Administrative and Professional Personnel Exchange Program (APEP) (see AR 70–41).

o. Manage the Army CPP Program (see AR 70–41).

p. Ensure foreign disclosure guidance on materiel items is provided to Training and Doctrine Command (TRADOC) in sufficient detail to support training course development and execution for foreign government trainees.

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

1–8. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

a. Appoint, in writing, a DA member to be the FDO, and FDRs, as appropriate.

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

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

e. 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.

f. Ensure the disclosure criteria cited in chapter 2 of this regulation are considered for each international program for which the DCS, G–3/5/7 has primary responsibility and which potentially involves the international transfer of CMI and CUI.

g. Assess implications of proposed disclosures and/or transfers on DCS, G–3/5/7 programs, plans, and policies.

h. Administer, manage, and implement the Army Military Personnel Exchange Program (MPEP) (see AR 614–10).

i. Oversee the American, British, Canadian, Australian, and New Zealand Armies interoperability program, including the standardization representative (StanRep) program.

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

k. Oversee Latin America Cooperation activities.

l. Ensure all first-time disclosures or denials of CMI by DCS, G–3/5/7 (DCS, G–3/5/7) are recorded in SPAN in compliance with this regulation and DODD 5230.11.

1–9. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Oversee logistics operations associated with security cooperation.

b. Appoint, in writing, a DA member to be the FDO, and FDRs, as appropriate.

c. Ensure all first-time disclosures or denials of CMI by DCS, G–4 (DCS, G–4) are recorded in SPAN in compliance with this regulation and DODD 5230.11.

1–10. Deputy Chief of Staff, G–8

The DCS, G–8 will—

a. Appoint, in writing, a DA member to be the FDO, and FDRs, as appropriate.

b. Serve as the DA proponent for modeling and simulation.

c. Identify and disseminate information regarding critical technologies in modeling and simulation that should not be transferred to foreign entities.

d. Ensure all first-time disclosures or denials of CMI by DCS, G–8 are recorded in SPAN in compliance with this regulation and DODD 5230.11.

1–11. The Judge Advocate General

TJAG will—

a. Provide a legal review of the DCS, G–2 and ASA (ALT) determination of whether adequate technical and contractual safeguards can be developed to preclude the inadvertent diversion of critical technology.

b. Appoint, in writing, a DA member to be the FDO, and FDRs, as appropriate.

c. Provide direct staff support to the Army member of the DOD Arms Transfer Working Group and the NDPC.

d. Review for legal sufficiency, all proposals regarding the establishment of international agreements, prior to initiation of any negotiations pursuant to such proposals.

e. Ensure all first-time disclosures or denials of CMI by TJAG are recorded in SPAN in compliance with this regulation and DODD 5230.11.

f. Ensure qualified personnel are available to provide legal advice on disclosure matters involving foreign governments, as required.

1–12. The Surgeon General, Chief of Engineers, and Chief Information Officer/G–6

TSG, COE, and CIO/G–6 will—

a. Ensure that foreign disclosure factors and implications are considered for each international program for which they have primary responsibility and which potentially involves the disclosure of CMI.

b. Appoint, in writing, a DA member to be the FDO, and FDRs, as appropriate.

c. For CIO/G–6: Formulate, establish, and disseminate policy and procedures for access to computers and computer networks, to include access by foreign representatives and nationals.

d. Ensure all first-time disclosures or denials of CMI by the Office of TSG, COE, and CIO/G–6 are recorded in SPAN in compliance with this regulation and DODD 5230.11.

1–13. Commanders, Army commands, Army service component commands, and direct reporting units

Commanders, ACOMs, ASCCs, and DRUs will—

a. Appoint, in writing, a DA member to be the FDO, and FDRs, as appropriate.

b. Publish ACOM, ASCC, or DRU guidance that will—

(1) Ensure all CMI and CUI being considered for foreign disclosure are referred to the FDO or FDR for appropriate coordination. The final CMI foreign disclosure decision will be in compliance with NDP–1 and this regulation. The final CUI foreign disclosure decision will be in accordance with this regulation.

(2) Ensure all first-time disclosures or denials of CMI by the command or DRU are recorded in SPAN in compliance with this regulation and DODD 5230.11.

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

d. Report and process violations of policies and procedures contained in this regulation in the manner prescribed for the compromise or potential compromise of CMI or CUI, as provided in AR 380–5. A copy of all such reports will be provided to DCS, G–2.

e. Appoint contact officers, in writing, for all extended official foreign visitors to all echelons of their agency or command.

f. Conduct annual onsite visits to organizations, agencies, activities, installations, and facilities over which ACOMs, ASCCs, or DRUs exercise administrative control or security cognizance to ensure compliance with this regulation.

1–14. Chief, National Guard Bureau

The CNGB will, in participation with the Army Staff, formulate, develop, and coordinate all foreign disclosure programs, policies, principles, concepts, and plans pertaining to or affecting the Army National Guard. By way of illustration, this includes but is not limited to, disclosures in support of the State Partnership Program. The CNGB will—

a. Appoint, in writing, a FDO and FDRs, as appropriate.

b. Publish NGB guidance that will—

(1) Ensure all Army CMI and CUI being considered for foreign disclosure are referred to the FDO or FDR for appropriate coordination. The final CMI foreign disclosure decision will be in compliance with NDP–1 and this regulation. The final CUI foreign disclosure decision will be in accordance with this regulation.

(2) Ensure all first-time disclosures or denials of Army CMI by the NGB are recorded in SPAN in compliance with this regulation and DODD 5230.11.

c. Provide support to combatant command and Army security cooperation programs as appropriate.

d. Report and process violations of policies and procedures contained in this regulation in the manner prescribed for the compromise or potential compromise of Army CMI or CUI, as provided in AR 380–5. A copy of all such reports will be provided to DCS, G–2.

e. Appoint contact officers, in writing, for all extended official foreign visitors to all echelons of their agency or command.

f. Conduct annual on-site visits to organizations, agencies, activities, installations, and facilities over which the NGB exercises administrative control or security cognizance to ensure compliance with this regulation.

1–15. Chief, Army Reserve

The CAR will—

a. Appoint, in writing, a FDO and FDRs, as appropriate.

b. Publish Army Reserve guidance that will—

(1) Ensure all Army CMI and CUI being considered for foreign disclosure are referred to the FDO or FDR for appropriate coordination. The final CMI foreign disclosure decision will be in compliance with NDP–1 and this regulation. The final CUI foreign disclosure decision will be in accordance with this regulation.

(2) Ensure all first-time disclosures or denials of Army CMI by the Army Reserve are recorded in SPAN in compliance with this regulation and DODD 5230.11.

c. Provide support to combatant command and Army security cooperation programs as appropriate.

d. Report and process violations of policies and procedures contained in this regulation in the manner prescribed for the compromise or potential compromise of Army CMI or CUI, as provided in AR 380–5. A copy of all such reports will be provided to DCS, G–2.

e. Appoint contact officers, in writing, for all extended official foreign visitors to all echelons of their agency or command.

f. Conduct annual on-site visits to organizations, agencies, activities, installations, and facilities over which the Army Reserve exercises administrative control or security cognizance to ensure compliance with this regulation.

1–16. Commanding General, U.S. Army Materiel Command

In addition to those responsibilities cited in paragraph 1–13, the 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. Ensure foreign disclosure guidance on materiel items is provided to TRADOC in sufficient detail to support training course development and execution for foreign government trainees.

1–17. Commanding General, U.S. Army Intelligence and Security Command

In addition to those responsibilities cited in paragraph 1–12 above, the CG, INSCOM will—

a. Provide counterintelligence and security support to Army activities involved in international technology transfer and foreign disclosure matters.

b. 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.

c. Conduct counterintelligence investigations into suspected acts of espionage, unauthorized removal and retention of CMI and CUI, and known or suspected unauthorized disclosure of CMI, to include military technology and R&D data on acquisition systems.

d. Provide DCS, G–2 with all incident reporting where foreign government representatives violate established Army security policies and/or procedures. Upon termination of operational or investigative interest, provide DCS, G–2 with a summary of information.

1–18. Commanding General, U.S. Army Criminal Investigation Command

The CG, USACIDC is responsible for investigating felony criminal cases that involve international technology transfer issues. In addition to those responsibilities cited in paragraph 1–13, 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 and Border Protection Service and Department of State regarding the enforcement of international technology transfer laws or regulations.

d. Provide DCS, G–2 with all incident reporting where foreign government representatives violate established Army security policies and/or procedures. Upon termination of operational or investigative interest, provide DCS, G–2 with a summary of information.

1–19. Commanders, Army commands outside the continental United States

a. Outside continental United States (OCONUS) ASCC commanders will use the policy guidance contained in this regulation to establish local policies and procedures governing interactions with foreign representatives and control of foreign visitors. These policies and procedures must include provisions for foreign government security assurances, visitor identification, and records of the disclosure of information that occur during these visits. Copies of these policies and procedures will be provided to DCS, G–2 upon request.

b. OCONUS ASCCs of geographic combatant commands are to adhere to combatant command policies and procedures insofar as such policies and procedures are consistent with applicable DA guidance. DCS, G–2 will be advised of any conflicts. Significant conflicts will be resolved at the DA and/or DOD level. In all circumstances, the disclosure of Army-originated CMI and CUI to foreign governments and foreign representatives will be in accordance with this regulation.

c. For this purpose, OCONUS ASCCs are: U.S. Army Europe, U.S. Army Pacific, and U.S. Army Africa.

1–20. Other outside continental U.S. Army activities

Other OCONUS Army activities assigned to, or under the operational control of, an OCONUS ASCC commander will adhere to the OCONUS ASCC 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 U.S., its friends and allies, face a world of complex challenges and great opportunities. Since the terrorist attacks of 2001, we have been engaged in conflict unlike those that came before. The U.S. has worked with its partners to defeat the enemies of freedom and prosperity, assist those in greatest need, and lay the foundation for a better tomorrow. The National Defense Strategy builds on lessons learned and insights from previous operations and strategic reviews and establishes five objectives: defend the homeland; win the long war; promote security; deter conflict; and win our nation's wars. The presence of American forces overseas is a profound symbol of the U.S. commitment to its allies and partners. The U.S. military presence plays a critical role in assuring allies and partners 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 partner nations. A primary objective of U.S. security cooperation is to help allies and partners 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 partners.

b. Role of foreign disclosure in United States National Defense Strategy. U.S. sharing of its military resources (such as CMI or CUI resident in technology and materiel) is a critical component of security cooperation. CMI is a national security asset. 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*. A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification in accordance with EO 13526, but is pertinent to the national interests of the U.S. or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

(2) *Public domain*. For the purposes of this regulation, unclassified information that does not qualify for the status of CUI, as described in paragraph 2–3*b*(1), is deemed to be actually or potentially in the public domain (in other words, suitable for disclosure to the public at large). All Army information must be reviewed prior to release to the public. The proponent for the disclosure of Army public domain information is the 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. For the purposes of this regulation, the Army applies these functional definitions to the identification and categorization of CUI as well. 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 or 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 drawings 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, and combustibles) 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 and/or 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 and/or 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 paragraphs 2–4*a*(2)(a) and 2–4*a*(2)(b).

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

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

(7) *Category 7 (North American Defense)*. North American Defense information is that which concerns plans, programs, projects, operations, and certain specific technical data pertaining to equipment directly related to North American defense, especially when it is originated by or under the mission and control of U.S. Northern Command (USNORTHCOM) or the North American Air Defense Command (NORAD). It includes but is not limited to—

(a) Plans and related documents prepared by combined U.S. defense agencies concerning the defense of the U.S.

(b) Plans and related documents prepared in combination with the Government of Canada, either binationally (that is, NORAD) or bilaterally (that is, between USNORTHCOM and Canada Command).

(c) Plans and related documents prepared in combination with the Government of Mexico and the Government of the Bahamas.

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

(e) Information revealing a vulnerability to the defense of North America, or the vulnerability or official appraisal of combat readiness of any unit or facility, or the effectiveness of North American Defense 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 are used by the Army to ensure consistency and 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. As a cautionary note, Army personnel are reminded that these charts do not automatically convey any foreign eligibility for information.

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 warranted by significant U.S. interests. Basic disclosure criteria, conditions, and limitations in paragraphs 2–6 and 2–7 must be fully satisfied. The DA organization 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 DCS, G–2, which reviews, coordinates, and submits the request to the NDPC (see app B).

d. ENDPs will not be granted to accommodate the assignment of FLOs, cooperative program and/or project personnel, and foreign exchange personnel.

2–6. Basic disclosure criteria

All disclosure determinations, whether they involve CMI or CUI, are adjudicated on a case-by-case basis. Additionally, proposed disclosure programs must be reviewed in their entirety in order to determine whether the disclosure of CMI is required at some point in the program. Central to this process is the evaluation of the proposed disclosure to ensure it satisfies the criteria stated below.

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

(1) *Political criteria.* Disclosure is consistent with U.S. foreign policy and national security objectives regarding the recipient foreign government or international organization.

(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 U.S.

(e) The political benefits that could accrue to the U.S.

(f) Whether or not the transfer helps the U.S. to obtain or secure base, transit, and overflight rights or access to strategic locations.

(g) Other countries to which the U.S. has transferred the item.

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

(i) Whether or not the U.S. is the first supplier of the item.

(j) The possibility that the item could fall into the hands of terrorists.

(k) The impact of the transfer on the country's economy.

(l) Whether or not the transfer establishes an unfavorable political precedent.

(2) *Military criteria.* Disclosure is consistent with military security objectives regarding the recipient foreign government or international organization.

(a) The degree of participation in collective security by the U.S.

(b) How the transfer would affect coalition warfare in support of U.S. policy.

(c) How the item would increase the recipient country's offensive or defensive capability.

(d) How the transfer would increase the capability of friendly regional forces to provide regional security to assist the U.S. in the protection of strategic lines of communication.

(e) How the transfer will strengthen U.S. or allied power projection.

(f) To what extent the transfer is in consonance with U.S. military plans.

(g) Whether or not the export is consistent with Army regional multinational force compatibility (MFC) 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 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 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?

(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 Army program been leveraged from another Army or other military department weapons program? If so, has the original Army or other military department weapons PM reviewed and rendered a recommendation on the request? The technology or information may not be listed as critical program information for one program, but may be identified as critical program information for another program.

(q) Are there any special considerations involved with the disclosure that requires coordination external to the Army? (For example, communications security (COMSEC), low observable, and cryptologic information.) 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?

(3) 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 DCS, 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 only be used for specified military-related purposes.

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.

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

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

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

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

(5) 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.

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

a. The disclosure of DA CMI or CUI 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 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.

d. If the FDO determines that CMI or CUI 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—

(1) 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.

(2) Refer all 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 DCS, G–2.

Section II
Authority to Disclose Classified Military Information, Controlled Unclassified 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 principal 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 their 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, delegated disclosure 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 MFC and have been approved according to AR 34–1, AR 550–51, or both.

1. CIO/G–6.

2. DCS, G–3/5/7.

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 cooperation related sales, cooperative production, 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 international cooperative R&D agreements approved under AR 70–41 and AR 550–51. Also included are items adopted for allied or friendly MFC.

1. ASA (ALT).

2. CIO/G–6.

3. DCS, G–3/5/7.

4. DCS, G–4.

5. DCS, G–8.

6. TSG.

(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 MFC 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.

1. ASA(ALT).

2. CIO/G–6.

3. DCS, G–3/5/7.

4. DCS, G–8.

(d) Category 4. Disclosures of Category 4 CMI (Production Information) must be approved by DCS, 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 MFC.

1. DCS, G–3/5/7.

2. TSG.

(f) Category 6. DCS, G–3/5/7 has authority to make disclosure determinations for Category 6 CMI (U.S. Order of Battle).

(g) Category 7. Disclosure determinations for Category 7 CMI (North American Defense) 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 recorded into SPAN in compliance with this regulation and DODD 5230.11.

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

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

2–9. Controlled unclassified information disclosure authority and delegation of authority

a. Authority. Authority to disclose CUI identified in DODD 5230.25 is delegated to the originator or proponent of that information. CUI disclosure decisions will be made using the same basic disclosure criteria (see paragraph 2–6) as that used for CMI disclosure decisions and will comport with any and all relevant laws, regulations, and/or policies pertaining to the specific type of CUI at issue.

b. Redelegation. ACOM, ASCC, and DRU commanders and agency heads are authorized to redelegate disclosure authority for CUI covered by this regulation, subject to any other relevant laws, regulations, or policies pertaining to the specific type of CUI at issue.

c. Notice of intent to disclose Army controlled unclassified information. ACOM FDOs will provide advance notification of intent to disclose CUI to the Army CUI originator. Army CUI originators will acknowledge receipt of disclosure notifications and provide responses within 15 calendar days from notification of intent to disclose. A non-response from the CUI originator by the 15 calendar day suspense will be considered a concurrence. In cases where the Army CUI originator denies a proposed disclosure, the original notice of intent to disclose and the originator's denial and justification must be forwarded to Headquarters, Department of the Army, DCS G–2 (DAMI–CDD), who will serve as the final arbiter for the CUI disclosure decision. Based on the country categories listed in the Department of the Army Security Cooperation Strategy, FDOs will adhere to the following timelines for advance notification:

(1) Global Core Partner: 60 calendar days prior to disclosure.

(2) Key Army Partner: 75 calendar days prior to disclosure.

(3) Regional Partner: 100 calendar days prior to disclosure.

(4) Special Interest Country: 135 calendar days prior to disclosure.

2–10. Delegation of disclosure authority letter

A DDL is a document issued by the DCS, G–2, a delegated disclosure authority, or authorized proponent establishing 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 and CUI to foreign governments or international organizations in support of approved Army or DOD international programs or operational activities. DDLs will be prepared in accordance with appendix D. Unless otherwise specified, all DDLs will have an expiration date not later than five years from the DDL's date of approval. 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). Authorities conveyed in any DDL are specific and restricted in applicability to the scope of the specific effort they support. Organizations are strictly prohibited from using or transferring disclosure authorities from one DDL to another.

a. Classified military information delegation of disclosure authority letter. A DDL that authorizes the disclosure of CMI will be prepared collectively by the host DA command or agency proponent for the international or operational 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 DCS, 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 the ASA (ALT) for appropriate staffing. DCS, G–2, or their designee, is the approval authority for all CMI DDLs and revisions to CMI DDLs. As a matter of policy, DCS, G–2 will not approve blanket or overarching DDLs, such as organizational DDLs submitted by an ACOM, ASCC, or DRU that authorize disclosure authority for all or portions of its major subordinate commands. Local FDOs may approve administrative modifications to CMI DDLs, such as a change of contact officer.

b. Classified unclassified information delegation of disclosure authority letters. With the exception of FLO DDLs, DCS, G–2, or their designee, grants ACOM, ASCC, and DRU commanders, or their designated representatives (for example, primary staff officers), PEOs, PMs, directors, and original classification authorities (OCAs) delegated authority to approve DDLs that only authorize the disclosure of unclassified information. This authority may not be redelegated. All approved CUI DDLs will be accompanied by an approval cover memorandum signed by the ACOM, ASCC, and/or DRU commander, or their designated representatives, PEOs, PMs, directors, or OCAs in order to establish authority and accountability. For the purposes of the policy specified in this paragraph, FDOs are not recognized as a designated representative with signature authority unless they are an authorized signature authority on behalf of the commander, PEO, PM, or director.

2–11. Responsibilities and establishment of foreign disclosure officers, foreign disclosure representatives, and contact officers

a. Foreign disclosure officer. A FDO is a DA member appointed to oversee and control coordination and approval of specific disclosures of CMI and CUI. FDOs will be of sufficient military or civilian rank to make disclosure decisions on behalf of their organization's commander. FDOs are authorized for appointment to the lowest command or agency level that is the proponent for Army-originated, Army-developed, or Army-derived CMI and that routinely discloses U.S. CMI to foreign governments or international organizations in support of approved Army international programs or operational activities. Foreign disclosure is an inherently governmental function, therefore contractor personnel may not perform the duties of a FDO.

(1) *Foreign disclosure officer appointments.* FDO appointments will be in writing. Notification of such appointments will be made to ACOMs, ASCCs, and DRUs which will provide DCS, G–2 a consolidated FDO list no later than 15 January annually. Additionally, ACOMs, ASCCs, and DRUs will certify that all personnel identified as FDOs have completed the required FDO certification training. FDOs or personnel within the security chain of command will not serve concurrently as contact officers for FLOs, foreign exchange personnel, or CPP participants.

(2) *Foreign disclosure officer training.* All FDOs are required to complete an Army Foreign Disclosure Officer Certification Course and provide proof of completion to HQDA, DCS, G–2 through the ACOM, ASCC, or DRU. Appendix F provides a reference list of frequently asked questions regarding foreign disclosure that all FDOs must be able to answer.

(3) Foreign disclosure officer responsibilities.

(a) Be thoroughly familiar with the provisions and requirements set forth in this regulation.

(b) Serve as the primary point of contact for all command, organization, and/or activity foreign disclosure issues to include those related to the International Visits Program and issues of misconduct.

(c) Prepare command, organization, and/or activity foreign disclosure education and training per paragraph 2–12.

(d) Ensure command, organization, and/or activity foreign disclosure related information posted in the SENTRY database is up to date.

(e) Obtain and maintain a FVS account on the Security Policy Automation Network located on the Secret Internet Protocol Router Network (SIPRNET) or seek a waiver from the DCS, G–2. Accounts may be requested from the DOD FVS office, email at DTSASPANSupport@dtsa.mil.

(f) Oversee the activities of all command, organization, and/or activity appointed FDRs.

b. Foreign disclosure representative. A FDR is an individual designated in writing who assists and advises the FDO on all disclosure matters. FDRs can be either DA members or Army-employed contractor personnel. FDRs may be appointed at any level of command to provide foreign disclosure assistance and recommendations. FDRs will not make CMI disclosure decisions. FDRs are required to complete an Army Foreign Disclosure Officer Certification Course. The authority for FDRs who are DA members to disclose CUI will be in accordance with local policies and procedures. FDRs who are contractor personnel will not make any disclosure decisions.

c. Contact officer. A contact officer is a DA member appointed in writing to oversee and facilitate all contacts, requests for information, consultations, access, and other activities of foreign nationals who are assigned to a DA component or subordinate organization as extended visitors. All personnel designated as contact officers are required to

complete an Army Contact Officer Certification Course and provide proof of completion to their servicing FDO. Contact officer responsibilities are outlined in appendix O.

2–12. Foreign disclosure training and education

a. General policy. Commanders and those DA officials who have disclosure authority and missions will establish foreign disclosure education programs. These programs will be aimed at promoting quality performance of foreign disclosure responsibilities by command personnel and will be tailored, as much as possible, to the specific involvement of individuals in the foreign disclosure program and the command's mission. The program will—

(1) Provide the necessary information and guidance to ensure the foreign disclosure effort is fully integrated into all facets of the command and/or organization's roles, functions, and missions that involve foreign participation.

(2) Ensure that all assigned personnel within the command and/or organization can apply foreign disclosure policies and concepts in a consistent manner that is relevant to the command and/or organization's roles, functions, and missions that involve foreign participation.

(3) Ensure that foreign disclosure actions and activities add value to the command and/or organization's roles, functions, and missions that involve foreign participation.

(4) Ensure that foreign disclosure actions and activities remain in the proper balance with respect to protecting critical technologies and information.

b. Briefings.

(1) *Initial foreign disclosure orientation*. All DA personnel upon assignment and in-processing will be provided an initial orientation. At a minimum, this orientation will include:

(a) The fact that the Army has a foreign disclosure program and it is required to support and implement Army, DOD and national policy; and U.S. law with respect to interaction with foreign governments and international organizations;

(b) That AR 380–10 governs foreign disclosure and contacts with foreign representatives;

(c) Fundamental disclosure principles such as methods of disclosure and the requirement for established delegated disclosure authority in order to effect disclosures; and,

(d) The name and contact information of the command and/or organization's FDO and/or FDRs.

(2) *Refresher training*. All DA employees, especially those who play a role in the foreign disclosure program, will be provided refresher training in their responsibilities regarding foreign disclosure at least once a year. The actual frequency and nature of continuing foreign disclosure education must be determined by the needs of the command's foreign disclosure program and the nature of the command personnel involved in the program. At a minimum, all personnel will receive annual refresher training that reinforces the policies, principles, and procedures covered in initial and specialized foreign disclosure training. Whenever foreign disclosure policies and procedures change, personnel whose duties would be impacted by these changes must be briefed regarding such changes as soon as possible.

2–13. 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 their designee is to receive and respond to all foreign disclosure requests for CMI. In the situations cited below, the DCS, G–2 or their 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, Australian, or New Zealand (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 ASA (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 Army service component commands of unified commands in channels specified in international agreements regarding combined planning, training and/or exercises, and operations are processed by the Army service 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 DCS, 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 FDO command channels to the HQDA staff agency, ACOM, ASCC, or DRU exercising program responsibility, unless disclosure authority has been delegated.

c. Coordination and development of disclosure recommendations and/or decisions.

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

(2) Comments and recommendations on issues related to the disclosure of CMI or CUI 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 1–5*e*(1) through 1–5*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; American, British, Canadian, Australian, and New Zealand (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, clearly identify the benefits to the Army in disclosing information classified at a higher level to satisfy the disclosure requirement.

(g) 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?

(h) Whether the issue requires coordination outside DA (for example, with the Office of the Secretary of Defense, other military Service components, industrial proprietary concerns, or other countries).

2–14. Army Technology Protection Program

The senior Army leadership and the acquisition community recognizes the significance of international technology transfer in attaining our national security goals and objectives and has instituted the requirement for all PMs to develop technology protection documents in support of their respective programs. 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 and/or security offices. The purpose of the PPP is to identify critical program information (CPI) to be protected and to create a management plan that outlines measures to be taken by the PM necessary to protect the 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. DODI 5200.39 and DA pamphlet (Pam) 70–3 provide guidance regarding the development of the PPP.

b. Technology assessment/control plan. The technology assessment/control plan (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 and/or security offices. In acquisition programs, the TA/CP is a required annex to the PPP and must be completed no later than milestone B. The 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 summary statement of intent (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 and/or security offices. The 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.

Chapter 3
Modes, Methods, and Channels for Classified Military Information Disclosures, Controlled Unclassified 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 or CUI be disclosed 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 and CUI 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) Army liaison officers, including StanReps, to foreign governments and international organizations.

(c) Other foreign representatives assigned to the DA workforce (see apps L through N, 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 or CUI.

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 determined from the U.S. perspective only.

a. Foreign visits to Department of the Army activities and Department of the Army contractors.

(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 in accordance with 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) *Methods 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 DCS, G–2, 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 their 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 the 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 existence and scope of any such authorization are to be reflected in area clearance-related communications prescribed in AR 55–46.

3–3. Department of the Army controlled unclassified information disclosed during visits

Disclosure of CUI 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 authorized to disclose CUI. CUI disclosures must be limited to that information authorized to be disclosed to accomplish the purpose of the visit. What is considered essential will be determined from the U.S. perspective only.

a. Foreign visits to Department of the Army activities and Department of the Army contractors in the continental United States.

(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 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) *Methods of disclosure*. CUI 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 originator, proponent, and/or 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. 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 Department of the Army 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 CUI, if such disclosure is mission essential. The existence and scope of any such authorization are to be reflected in area clearance-related communications prescribed in AR 55–46.

3–4. Department of the Army classified military information or controlled unclassified information disclosed to foreign liaison officers, foreign exchange and cooperative program personnel

See paragraphs 3–2 through 3–3 and appendixes J through N for detailed information.

3–5. Documentary requests for United States classified military information and controlled unclassified information

Most disclosures of DA CMI and CUI occur through the direct personal interaction described above in paragraphs 3–1 through 3–4. 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 or CUI in documentary form. They are submitted to DCS, G–2 unless DCS, 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 or CUI documents regarding the provision of defense articles and services (including publications) will be submitted or referred to AMC and/or U.S. Army Security Assistance Command (USASAC) through established security assistance channels. On receipt, AMC and/or 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 DCS, G–2 for actions involving disclosure authority above that delegated to the command or agency. This action will be pursuant to AR 12–1 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 the requester's involvement in the agreement is authentic and 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 Accession-numbered document requests by the governments of Australia, Canada, and the United Kingdom. Since that time, additional 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 upon 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 first-time disclosure or denial, to DCS, G–2 for a final determination. Upon rendering a final decision, DCS, 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 paragraphs 3–5*a* through 3–5*c*, will be initiated by the embassies according to table 3–1 and the accompanying notes. When the instructions contained in table 3–1 direct the request be sent to DCS, 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 DCS, 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 DCS, G–2 of the final decision.

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

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

(d) In all cases, DCS, G–2 will administratively close the case upon the rendering of an approved final decision.

(5) For requests involving proprietary data—

(a) Return the request to the originating foreign embassy and inform the requesting embassy to submit the request to the owner of the proprietary data, or;

(b) Forward the request to the owner of the proprietary data for action and provide a copy of the letter to the requesting embassy; or;

(c) 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.

(d) The FDO will notify DCS, G–2 of the action taken to close the case.

(6) If the fulfillment of the request only requires the disclosure of CUI, the originator or proponent will—

(a) If approved, mark the document and forward it through the FDO to the requesting embassy, according to section II of this chapter. The FDO will notify DCS, G–2 of the final decision.

(b) If denying the request, forward the document and justification for denial through the FDO to DCS, G–2 for a final decision.

(c) In all cases, DCS, G–2 will administratively close the case upon the rendering of an approved final decision.

Section II
Administrative Procedures

3–6. Concept

Before DA CMI or CUI 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 or CUI 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 with respect to U.S. stated goals and objectives.

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. Prohibit the disclosure of other U.S. agency CMI or CUI without approval, in writing, from the originator or proponent.

f. Remove or obliterate all distribution lists and bibliographic data (bibliographies, lists of references, bibliographic notes).

3–7. 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 in accordance with the requirements of AR 380–5.

3–8. 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 decision makers and analysts in reviewing, coordinating, and rendering decisions or recommendations regarding proposals requiring the disclosure of CMI to foreign governments and international organizations. By recording these entries, SPAN can provide a tracking mechanism of the foreign disclosure of all Army CMI. It also can serve as a retrieval tool that can be used to present a comprehensive picture of the disclosures of 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 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 present justification for the disclosure. 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 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 with SPAN terminals will record the entry online. Those without an online SPAN capability will make their entries through the Foreign Disclosure System (FDS), which has a 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.

3–9. Foreign access to computers and computer networks

The provisions of AR 25–2 will govern access to Army computer systems (stand-alone or network), to include the Non-Secure Internet Protocol Router Network (NIPRNET) and the SIPRNET by FLOs and other foreign officials certified and assigned to Army organizations as well as official foreign government visitors. Disclosure of CMI and CUI through 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 Government Printing Office (GPO) or National Technical Information Service (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, AR, DA Pam, circular, and field manual).	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 DCS, 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 not certified to HQ, AMC.	(N/A)	Submit written request to USASAC.
4.	Contained in 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.)
6.	Maps and geospatial products.	(N/A)	(N/A)	Acquire the information from the National Geospatial Intelligence Agency, https://www1.nga.mil/Pages/Default.aspx
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).

Table 3–1
Document request procedures—Continued

10.	Other than those cited in items 1–9.	(N/A)	(N/A)	Submit written request to DCS, G–2.

Notes:

[1] Addresses for the GPO and the NTIS are: Superintendent of Documents, Government Printing Office, 710 North Capital Street, NW, Washington, DC 20402–0001, and National Technical Information Service, 5301 Shawnee Road, Springfield, VA 22312.

[2] Countries that are eligible to enter into FMS arrangements with the Army may be eligible to establish a FMS publications account with the 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 Army equipment and materiel under the auspices of FMS also may be referred directly to The Commander, U.S. Army Security Assistance Command (DRSAC–SC), 7613 Cardinal Road, Redstone Arsenal, Alabama 35898.

[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, Administrative Guidance provided to all embassies by HQDA.

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

Chapter 4
Technology Protection Program

4–1. Concept

a. This chapter describes the significance and the attention devoted to foreign disclosure's role in the Army's technology protection program. The senior Army leadership recognizes the role foreign disclosure plays in technology protection and has established the SENTRY disclosure decision support system as a means to facilitate the management of this responsibility.

b. The SENTRY foreign disclosure support system provides a secure, Web-based application that promotes a common operational picture for the Army foreign disclosure community and compliments and enforces existing DCS, G–2 Foreign Disclosure Branch, business processes.

c. The primary purpose for SENTRY is to serve as DA's official repository for all DA DDLs and certified visitors. Secondary uses of SENTRY include: providing the FDO Community with relevant information needed to address basic disclosure criteria when rendering disclosure decisions; and serving as a library for various resources (for example, security classification guides; directives, regulation, and guidance; program security documentation; National Disclosure Policy Records of Action; information on misconduct by visiting foreign representatives; and so forth) useful in the development of disclosure guidance.

4–2. SENTRY requirements

a. All FDOs and FDRs are required to have an active SENTRY account. FDOs will be responsible for validating that their subordinate unit FDO nominees for a FDO SENTRY account have successfully completed an Army FDO Certification Course and have been appointed as a FDO in accordance with this regulation.

b. Army activities will record all RFIs submitted by FLOs and a summary of all official information provided by FLOs in SENTRY within twenty business days of the transaction.

c. Army activities will post all extended visitor terms of certification to SENTRY within ten business days of approval.

d. The DCS, G–2 will post DDLs to SENTRY within ten business days of approval.

Appendix A
References

Section I
Required Publications

AR 380–5
Department of the Army Information Security Program (Cited in paras 1–5a(1), 1–5f(2), 1–5f(4), 1–5f(7), 1–5f(11), 1–12d, 1–13d, 1–14d, 1–15d, 2–3a, 3–2a(3), 3–3a(3), 3–7, G–1, P–4b(1), P–4u.)

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations (Cited in paras 1–5c, 1–5i, 1–7l, 1–8c, 1–9d, 1–10e, 1–11d, 1–12b(2), 1–13b(2), 1–14b(2), 1–15b(2), 2–8b(2), D–2a, P–4b(2).) (Available at http://www.dtic.mil/whs/directives.)

DODD 5230.20
Visits and Assignments of Foreign Nationals (Cited in paras 1–5c, 1–5j, D–2a, I–6a, I–6b, J–2a, J–2b, P–4b(3).) (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. Department of Defense regulations are available at http://www.dtic.mil/whs/directives. United States Codes and Code of Federal Regulations are available at http://www.gpo.gov/fdsys/.

AECA
Arms Export Control Act (22 USC 2778–2780) (Available at http://www.pmddtc.state.gov/regulations_laws/aeca.html.)

AR 5–11
Management of Army Models and Simulations

AR 10–87
Army Commands, Army Service Component Commands, and Direct Reporting Units

AR 11–2
Managers' Internal Control Program

AR 11–31
Army Security Cooperation Policy

AR 12–1
Security Assistance, Training, and Export Policy

AR 12–15
Joint Security Cooperation Education and Training

AR 25–2
Information Assurance

AR 25–30
The Army Publishing Program

AR 25–50
Preparing and Managing Correspondence

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
Multinational Force Compatibility

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 70–41
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
Personal Commercial Solicitation on Army Installations

AR 340–21
The Army Privacy Program

AR 360–1
The Army Public Affairs Program

AR 380–28 (C)
The Department of the Army Special Security System (U) (Available at http://www.dami.army.smil.mil/site/daispom/pub/ar380–28.pdf.)

AR 380–40
Safeguarding and Controlling Communications Security Material

AR 380–67
Personnel Security Program

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 381–12
Threat Awareness and Reporting Program

AR 381–20
The Army Counterintelligence Program

AR 420–1
Army Facilities Management

AR 530–1
Operations Security (OPSEC)

AR 550–51
International Agreements

AR 614–10
Army Military Personnel Exchange Program with Military Services of Other Nations

DA Pam 70–3
Army Acquisition Procedures

Defense Acquisition Guidebook
Section 11.2, Considerations for International Cooperation (Available at https://dag.dau.mil/Pages/Default.aspx.)

DIA Regulation 50–27 (C)
Disclosure of Collateral Military Information to Foreign Governments and International Organizations (Available at the Secret Internet Protocol Router Network at http://www.dia.smil.mil/admin/REG–MAN/r50–27/r50–27_intro.html.)

DOD 5105.38–M
Security Assistance Management Manual (SAMM)

DOD 5220.22–M
National Industrial Security Program Operating Manual

DODM 5200.01
DOD Information Security Program: Controlled Unclassified Information

DODD 4500.54E
DOD Foreign Clearance Program (FCP)

DODD 5100.55
United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)

DODD 5230.25
Withholding of Unclassified Technical Data From Public Disclosure

DODD 5400.07
DOD Freedom of Information Act (FOIA) Program

DODD 5530.3
International Agreements

DODI 2010.06
Materiel Interoperability and Standardization with Allies and Coalition Partners

DODI 2015.4
Defense Research, Development, Test and Evaluation (RDT&E) Information Exchange Program (IEP)

DODI 2040.02
International Transfers of Technology, Articles, and Services

DODI 3200.14
Principles and Operational Parameters of the DOD Scientific and Technical Information Program

DODI 5000.02
Operation of the Defense Acquisition System

DODI 5200.01
DOD Information Security Program and Protection of Sensitive Compartmented Information

DODI 5200.39
Critical Program Information (CPI) Protection Within the Department of Defense

DODI 5230.24
Distribution Statements on Technical Documents

EAR
Export Administration Regulations (15 CFR 768 et seq.) (Available at http://www.access.gpo.gov/bis/ear/ear_data.html.)

Executive Order 13526
Classified National Security Information (Available at http://www.archives.gov/federal-register/index.html.)

ITAR
International Traffic in Arms Regulation (22 CFR 120–130) (Available at http://www.pmddtc.state.gov/regulations_laws/itar.html.)

Military Attaché Guide
(Available at http://www.dami.army.pentagon.mil/DAMI–FLGuide.aspx.)

MCTL
Militarily Critical Technologies List (Available at http://www.dtic.mil/dtic/stresources/standards/mctl_desc.html.)

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 DCS, G–2.)

Public Law 104–201
National Defense Authorization Act for Fiscal Year 1997

8 USC 1101
Definitions

8 USC 1157
Annual admission of refugees and admission of emergency situation refugees

8 USC 1158
Asylum

8 USC 1160
Special agricultural workers

8 USC 1255a
Adjustment of status of certain entrants before January 1, 1982 to that of person admitted for lawful residence

8 USC 1324b
"Protected individual" defined

10 USC 168
Military to Military Contacts and Comparable Activities

10 USC 2667
Leases: non-excess property of military departments and Defense Agencies

10 USC 2675
Leases: foreign countries

22 USC 2796
Leasing Authority

50 USC 2410
Violations

50 USC 2411
Enforcement

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the APD Web site (http://www.apd.army.mil) and DD Forms are available on the Office of the Secretary of Defense Web site (http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DTIC Form 55
Defense Technical Information Center Request for Release of Limited Document

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, or;

(2) Does not comply with any of the basic disclosure criteria and conditions prescribed in chapter 2 of this regulation, or;

(3) Exceeds or does not comply with disclosure guidance issued in NDPC Policy Statements.

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 DCS, 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 DCS, G–2.

Note. Due to classification, all electronic ENDP activities will be carried out on SIPRNET.

c. DCS, G–2 or their 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 a Record of Action. DCS, G–2 will, at a minimum, disseminate the decision, with accompanying disclosure guidance, to the HQDA proponent, the initiator of the request, the appropriate ACOM, ASCC, or DRU and USASAC (if applicable), and post to SENTRY.

B–2. Exception to the National Disclosure Policy request format
A sample format for an ENDP request is at figure B–1.

(CLASSIFICATION)
DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 ARMY PENTAGON
WASHINGTON DC 20310-1000

DAMI-CDS (DATE)

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

SUBJECT: Request for an Exception to the National Disclosure Policy – (Insert country here) (Army NDPC Case Number 2###-YR) (U) (Case numbers input by ODCS, G-2)

1. (*) The Department of the Army requests an exception to the National Disclosure Policy (NDP-1) to permit the disclosure of (insert CLASSIFICATION) Category (insert one or more NDP-1 categories, each with its designation, for example, Category 2 (Military Materiel and Munitions)) information to the Government of (insert country) (remainder of the 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 negotiations of a Data Exchange Agreement pertaining to (technology)"). The remainder of the paragraph will be filled in by ODCS, G-2 as lead agency with the requestor as assist.

2. (*) Explain why the exception is required. Usually, an exception is required for one or any combination of the following three reasons: a) Army has not been delegated disclosure authority at the necessary classification level for that country in Annex A of NDP-1; or b) the proposed disclosure is not in consonance with policy currently established in Annexes B or C of NDP-1; or c) the disclosure criteria or conditions (identify which) listed in Section II of NDP-1 are not fully met. Sample language for this paragraph is "An exception is required because the level of classified military information proposed for disclosure exceeds that delegated in Annex A, NDP-1 for (insert country)."

3. (*) If applicable, address the background behind the request. For example, "In July 2010, the Government of (insert country) submitted a Letter of Offer and Acceptance for the Lightweight Counter-Mortar Radar (LCMR). Previously managed by USSOCOM, the LCMR is now an Army program. In response to urgent past operational requirements, USSOCOM and the Army supported sale of the system to the United Kingdom, Australia, and Canada. This transfer via Foreign Military Sales is fully endorsed by the U.S. Embassy country team and U.S. (combatant command)."

4. (*) A description of the information to be disclosed. For example: "The M830A1 HEAT-MP-T is a multi-purpose round designed to attack ground and limited air targets.

CLASSIFIED BY:
DERIVED FROM:
DECLASSIFY ON:

(CLASSIFICATION)

Figure B–1. Exception to the National Disclosure Policy format

(CLASSIFICATION)

It consists of a Body Assembly (shaped charge), M74 Proximity Switch (radar sensor), M774 Fuze, Fin and Tracer, Propelling Charge and Combustible Cartridge Case. The M830A1 is fired from the M256 Gun mounted on the M1A1 and M1A2 Abrams tanks. It can engage a variety of targets in its ground mode and helicopters in its air-burst mode."

a. (*) Describe the system. Designate exactly what you are trying to disclose.

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

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

a. (*) Disclosure is consistent with U.S. foreign policy and military objectives concerning (insert country).

(1) (*) State whether or not the U.S. country team supports the 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 will be consulted concerning the approval. Attach as an enclosure a copy of the country team correspondence that provides it comments. Sufficient time should be allowed to obtain an opinion from U.S. Embassy personnel in country before submitting the request. Many cases are delayed because a U.S. Embassy opinion has not been obtained.) ODCS, G-3 (lead); ODCS, G-2 (assist).

(2) (*) Cite any U.S. policies or military objectives, avoiding generalities such as "the recipient cooperates with the United States in pursuance of military or political objectives." The following political and military considerations should be addressed:

Political Considerations:

(*) The potential foreign recipient's support for U.S. foreign policy and political objectives.

(*) The potential of the transfer to deny or reduce an influence or presence in the country that is hostile to U.S. interests.

(*) The effects on the regional and global strategic balance if the transfer is approved.

(*) Whether or not the country has a defense treaty or political agreement with the United States.

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

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

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

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

(*) Whether or not the United States is the first supplier of the item.

(*) The possibility that the item could fall into the hands of terrorists.

(*) The impact of the transfer on the country's economy.

(*) Whether or not the transfer establishes an unfavorable political precedent.

(CLASSIFICATION)

Figure B–1. Exception to the National Disclosure Policy format—Continued

(CLASSIFICATION)

Military Considerations

(*) The degree of participation in collective security by the United States.

(*) How the transfer would affect coalition warfare in support of U.S. policy.

(*) How the item would increase the recipient country's offensive or defensive capability.

(*) 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.

(*) How the transfer will strengthen U.S. or allied power projection.

(*) To what extent the transfer is in consonance with U.S. military plans.

(*) Whether or not the export is consistent with Army regional MFC policy.

(*) Whether or not the system or item is a force structure requirement.

(*) Whether or not the country's technology base can support the item.

(*) To what degree the system or item counters the country's threat.

(*) to what extent the system constitutes part of an appropriate force and systems mix.

(*) 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 requestor (lead): OASA(ALT) and ODCS, G-2 (assist).

(1) (*) 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?

(2) (*) Do the PM and OASA(ALT) support the disclosure of this system (if they are not the ENDP requestor)?

(3) (*) 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?

(4) (*) 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?

(5) (*) If there is a security classification guide for the system and it is not in SENTRY, it should be attached as an enclosure.

(6) (*) 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 by the following:

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

(CLASSIFICATION)

Figure B–1. Exception to the National Disclosure Policy format—Continued

(CLASSIFICATION)

(2) (*) Industrial security agreement, if applicable. (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, if applicable. (Same guidance as in (1), above.)
(6) (*) (Add additional information to describe the security situation that pertains to the foreign recipient. Disclosures of other U.S. CMI to that country may be cited 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, combined exercise, or operation 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 information) or Production (Category 4 information) data is not involved or that documentation will be sanitized.) Initial requestor (lead); ODCS, G-3 and ODCS, G-2 (assist).

6. (*) Explain any conditions or 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 requestor (lead); OASA(ALT) and ODCS, G-2 (assist).

7. (*) State whether the exception is a continuing exception, subject to annual review (or is a one-time exception to expire on a given date). (A continuing exception is usually associated with a long-term project, such as an operation, a coproduction program, or foreign military sale when the United States will be obligated to provide life cycle support. A one-time exception typically is used for briefing or demonstration or short-term training.) Initial requestor (lead); OASA(ALT) and ODCS, G-2 (assist).

(CLASSIFICATION)

Figure B–1. Exception to the National Disclosure Policy format—Continued

(CLASSIFICATION)

8. (*) Request a vote on this exception by (insert date). (Ten full working days should be allowed for NDPC case deliberations. The suspense date is computed starting from the first full working day after the date of submission to the NDPC Secretariat.)

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 request at issue. Initial requestor (lead); OASA(ALT) and ODCS, G-2 (assist).

Encls

Signature Block
Army Member
NDPC

(Recommended enclosures: Country team correspondence, foreign country request, security classification guide (if applicable), political/military assessment, 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.

NOTE: All sources of security classification must be listed on a separate page at the end of the request. The security classification guide for NDP-1 is found in DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations.

Figure B–1. Exception to the National Disclosure Policy format—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 servicing

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. The TA/CP and SSOI are the primary source documents for preparation of the DDL to support international agreements and foreign government or international organization involvement in Army acquisition programs.

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 and/or Army security policies and procedures.

Appendix D
Delegation of Disclosure Authority Letter

D–1. General

a. 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. The DDL serves as the cornerstone of the disclosure program from both an authoritative and administrative perspective. As such, it needs to be specific and relevant to the required purpose. DCS, G–2, delegated disclosure authorities, and authorized proponents, approve and issue DDLs for programs or projects regarding the following:

(1) International agreements.

(2) FLOs.

(3) Army personnel exchange programs (PEPs), ESEPs, and CPPs.

(4) Weapon systems.

(5) Organizations.

(6) Cooperative R&D (that is, DEAs, technology research and development programs (TRDPs), The Technology Cooperation Programs (TTCPs), and so forth).

(7) Requests for proposals (RFPs).

(8) Combined military operations and exercises.

b. All DDLs will expire not later than five years after the date of approval or upon conclusion of the activity requiring disclosures, whichever occurs first.

D–2. Requirement

a. 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 Army weapons acquisition programs, international agreements, and FLO, StanRep, PEP, ESEP, and CPP positions. This requirement applies to the above-mentioned international programs regardless of whether access to CMI is involved.

b. An approved DDL is required to be in place prior to a commitment to assign a FLO, exchange program participant, CPP participant, or Country Liaison Officer (CLO) to a DA component. A DDL is also required to support disclosures of CMI during combined operations or exercises.

c. With the exception of FLO DDLs, ACOM, ASCC, and DRU commanders, or their designated representatives, PEOs, PMs, directors, and OCAs may approve DDLs that only authorize the disclosure of unclassified information. However, a hardcopy version of the document, accompanied by an approval cover memorandum signed by the ACOM, ASCC, or DRU commander, or their designated representative, PEO, PM, director, or OCA, must be furnished to DCS, G–2 within ten working days of approval and signature. If the ACOM, ASCC, or DRU commander, or their designated representative, PEO, PM, director, or OCA exercises their authority to approve a DDL that only authorizes the disclosure of unclassified information, the organization may assign a case number and/or designator to the DDL. An example of an appropriate case number would be "E–AMC–GE–001," which represents the program identification (F=operational FLO, S=security assistance FLO, M=MPEP, E=ESEP, or C=CPP), ACOM, two-letter foreign country code, and number. However, the DCS, G–2 will assign the Army DDL designator which is auto-generated by the SENTRY database.

d. Commands submitting DDLs to DCS, G–2 for approval will ensure the DDLs submissions include all supporting documentation. Examples of supporting documentation include, but are not limited to: TA/CPs; SSOIs; security classification guides; program protection plans; copy of the international agreement supported by the DDL; and approved extended visitor position descriptions.

D–3. Position delegation of disclosure authority letters

a. Position delegation of disclosure authority letters. Position DDLs will be established to facilitate the assignment of foreign representatives to positions in DA organizations that will not likely change over time. These positions usually apply to the assignment of FLOs and exchange personnel to DA organizations. Position DDLs are also applicable to Guest Instructors and CLOs under the provisions of AR 12–15 and Instructor Pilots under the provision of established international agreements.

b. Position delegation of disclosure authority letters that authorize the disclosure of classified military information. DA host organizations will conduct a review of foreign representative assignment positions and DDLs at least 90 days prior to the scheduled departure of the incumbent. Upon completion of the review, the DA host organization may revalidate the position and recommend revalidation of the existing DDL for the replacement person (see appendix 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 extended visit authorization (EVA) submitted by the replacement person's parent embassy in Washington, DC, DCS, G–2 will simultaneously approve the revalidation of the existing position DDL. Upon approval of the DCS, G–2, the DA host organization, through the FDO, will incorporate 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. With the exception of FLO DDLs, 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 ACOM, ASCC, or DRU commander, or their designated representative, PEO, director, or OCA may exercise their authority to approve the supporting DDL provided it only authorizes the disclosure of unclassified information (see para D–4). The ACOM, ASCC, or DRU commander, or their designated representative, PEO, director, or OCA 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 a FLO position). A copy of the approved DDL along with the signed approval cover memorandum will be provided to DCS, G–2 according to the procedures cited in paragraph D–4. Upon receipt of the approved DDL, the DCS, G–2 will then render a decision regarding the EVA 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

a. 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. The DDL is a dynamic document that must be tailored to service the program or event for which it is written. 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 4 of the DDL as a disclosure authority for that DDL. Upon receipt of the 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. All approved DDLs must be accompanied by a signed approval cover memorandum. DDLs that lack a signed approval cover memo are unapproved DDLs and will not be used as the authority to disclose Army information. Formatting of the DDL will be in accordance with AR 25–50.

b. At a minimum, a DDL consists of the following eight elements. They should be provided in the order shown and information should be presented in the clearest and easiest-to-use manner. Some DDLs, such as those dealing with people or exercises, will have more than eight elements (for example, Contact Officer, Visit Procedures). For complex weapon system DDLs, consideration should be given to breaking out paragraphs 5 and 6 by major sub-systems to enhance the usefulness of the DDL. Additionally, system DDLs must include disclosure guidance for the system in a tactical environment. In all instances, the final paragraph of the DDL will be the redelegation paragraph.

(1) *Classification.* This paragraph indicates the highest level of classification ("Unclassified," "Controlled Unclassified," "CONFIDENTIAL," "SECRET," or "TOP SECRET") of information that is authorized for disclosure in support of the program or event. This level must take into account both the various categories of CMI and the country(ies) involved. This stated classification level does not obligate disclosures at this level, but rather gives authority to do so as the mission requires.

(2) *Disclosure Methods.* This paragraph indicates the medium in which the information can be disclosed. There are

three types of disclosures: oral, visual and documentary. Disclosure methods can be any combination of the three and depend on the nature of the program or event.

(a) Oral disclosure. Refers to the ability to convey information through conversation. The limiting factor is that information that can be conveyed through speech.

(b) Visual disclosure. Refers to the ability to actually show the information. Visual disclosure also allows study and analysis of the information.

(c) Documentary disclosure. Refers to the ability and authority to convey permanent physical custody of the information to be disclosed. Disclosures of information for temporary purposes, such as information required by a PEP consistent with their position description, is not a documentary disclosure. The PEP may not retain permanent custody of the information when their term expires.

(3) *Categories Permitted.* This paragraph identifies which of the eight NDP–1 categories of CMI or other types of information may be disclosed. The eight NDP–1 categories will also be used for those DDLs only authorizing the disclosure of unclassified information.

(4) *Scope.* This paragraph serves the function of establishing applicability. It specifies who is authorized to disclose the material or information, and, in some instances, to whom disclosure is authorized and under what conditions. It can be used to describe an event (for example, a combined exercise) or a position description of an extended visitor such as a FLO, PEP, ESEP, or CPP. Additionally, the Scope paragraph can address associated installations, agencies, or commands which may be pertinent to the program or event to be included in the disclosure authorization. CMI disclosure authority is generally restricted to original classification authorities.

(5) *Authorized for Disclosure.* As precisely as possible, describe the material or information under the cognizance of the disclosure authority cited in the Scope paragraph that can be disclosed. Specify any conditions or limitations to be imposed (for example, time-phasing of disclosure, allowable forms of software, identification of items releasable only as finished, tested items). Information listed in this paragraph as being authorized for disclosure must be consistent with the categories of information listed in paragraph 3 of the DDL. For every category of CMI requested in paragraph 3 of the DDL, at least one specific example of that type of information must be cited in this paragraph.

(6) *Not Authorized for Disclosure.* This paragraph specifies the limits of the disclosure authority. It describes material or information that cannot be disclosed. This paragraph is usually broken into two subparagraphs:

(a) General. Information of a general nature which is normally not disclosed. Entries under this category are dependent on the type of DDL being written.

(b) Specific. Specific items listed as not authorized for disclosure must be indicated at the same level of detail as information listed in paragraph 5 of the DDL. Particular attention must be paid to the protection of CPI, if applicable.

(7) *Procedures.* This paragraph captures the business rules of the disclosure program. It specifies the requirements for things such as, review and transfer procedures, access to automation systems and networks, visit procedures, as well as special security procedures or protective measures to be imposed, recording CMI disclosure decisions, the requirement, if any, for coordination both within Army and with outside agencies.

(8) *Redelegation.* Specifies the extent of redelegation of disclosure authority, if any, permitted to subordinate activities. In general, CMI disclosure authority may not be redelegated (see para 2–8*b*(4)). When additional paragraphs are required in the DDL (for example, Contact Officer, Visit Procedures), the redelegation paragraph is always the last paragraph of the DDL.

c. DDLs that support extended visitors (that is, FLO, PEP, CPP) will have a paragraph that identifies the responsibilities of the DA members who have been assigned as primary and alternate Contact Officers for the extended visitor. Contact Officer responsibilities can be found in appendix O.

d. The name, duty assignment, duty phone number, and duty address of the primary Contact Officer and any alternate Contact Officer(s) will be prepared as an enclosure to the DDL.

D–5. Warning statement

a. From an administrative perspective, each DDL requires a warning statement stipulating that the DDL is an internal 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.

b. The warning statement is to be placed at the top and bottom of each page of the DDL. The warning statement must be upper case, bold and in a larger font than the contents of the document so that it clearly stands out. The warning statement text is as follows: "THE INFORMATION CONTAINED IN OR A COPY OF THIS DDL WILL NOT BE DISCLOSED TO ANY FOREIGN GOVERNMENT OR FOREIGN REPRESENTATIVE."

c. Additionally, the appropriate classification will be placed at the top and bottom of each page in accordance with current classification marking guidance. Minimum classification of all DDLs is "UNCLASSIFIED//FOR OFFICIAL USE ONLY."

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

SUMMARY STATEMENT OF INTENT FOR INTERNATIONAL RESEARCH AND DEVELOPMENT AGREEMENT

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 MOU or other international agreement in effect that is applicable to this effort?
   b. Is this proposed for nunn funding? If so, what technological development is to be pursued which is necessary to develop new defense equipment or munitions, or what existing military equipment would be modified to meet U.S. requirements?

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 Arms Export Control Act (AECA), Section 27 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 U.S.** List the advantages and disadvantages of this cooperative project. Address project timing, developmental and life cycle costs, technology to be shared and obtained, impact on U.S. and foreign military capability, and rationalization, standardization and interoperability considerations. Indicate whether there are any risks associated with conducting this project as an international cooperative program, and briefly describe how these risks are to be managed. Is a

Figure E–1. Summary Statement of Intent

similar project currently in development or production in the U.S. or an allied nation? If so, could that project satisfy or be modified in scope to satisfy the U.S. requirement?

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 U.S.? Are you aware of any key parts or components with a single source of production? What USG facilities and/or contractors would be likely to participate in this cooperative effort? Will there be any significant effects (pro or con) on any U.S. companies or U.S. industrial sector(s)?

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 non-financial contributions included in the cost shares.

c. If not equitable financially, justify on a program basis (show relative benefit to the Department of Defense). An equitable agreement is defined as one in which a participant's share of contributions to an agreement is commensurate with that participant's share of anticipated benefits from the agreement.

d. List the Department's estimated costs by fiscal year, appropriation, and program element. Indicate if these costs have been, or will be, approved in the budget and are available for use.

e. List other participants' estimated costs by fiscal year.

f. If applicable, outline the likelihood of follow-on research or acquisition and the proponent's commitment to fund such follow-on action.

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 Transfer 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. Is an exception required to the NDP? If so, provide date of approval or date that a request will be submitted to the National Disclosure Policy Committee.

c. If known, describe the foreign availability of comparable systems and technologies and whether the U.S. technology has been shared through other programs, for example, FMS and DEA.

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

Figure E–1. Summary Statement of Intent—Continued

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

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 RAD review period.

Figure E–1. Summary Statement of Intent—Continued

Appendix F
Frequently Asked Questions, Corresponding Answers, and Applicable References

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 table F–1.

Table F–1.
Frequently asked questions

Question: What is proprietary information?
Answer: Classified or unclassified information, the rights to which are owned by private firms or citizens (such as patents, copyrights, and trade secrets) (see para 1–5f(15) and glossary).

Question: Which officials have the authority to approve DDLs?
Answer: DDLs, depending on the classification level of information to be disclosed, are approved by the DCS, G–2, ACOM, ASCC and DRU commanders, or their designated representatives (for example, Primary Staff Officers), Program Executive Officers (PEOs), Program Managers (PMs), Directors and original classification authorities (see para 2–10). DCS, G–2, or their designee, is the approval authority for all CMI DDLs or revisions thereto.

Question: May a FLO have access to DDLs?
Answer: DDLs are intended for internal Army use only and will not be provided to, nor will their contents be disclosed to, foreign representatives (see para 2–10).

Question: Under a DDL, may a FDO disclose CMI that was classified by another original classification authority?
Answer: Yes, provided the original classification authority also has regulatory authority or a DDL and has authorized the specific disclosure in writing. See paragraph 2–8 for HQDA agency heads and the specific DDLs for ACOM commanders, 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 their program.

Question: Which AR governs access to computers by a foreign government representative?
Answer: AR 25–2

Question: Why is recording the first-time disclosures of CMI in the SPAN important?
Answer: Recording first-time disclosures, SPAN provides a tracking mechanism of the foreign disclosure of all Army classified information (see para 3–8).

Question: Should DDLs be disseminated outside of FDO channels?
Answer: Yes. DDLs should be disseminated to all affected parties (see para D–4a).

Question: How do you handle visits of foreign nationals who are not representing their respective parent government to Army commands or agencies?
Answer: See paragraph 1–5g. 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 foreign citizens, 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: Expenditure of DA funds and/or resources in support of foreign representative visits may be authorized under certain circumstances. Care should be taken to ensure that the nature of the visit is such that the specific expenditure of DA funds or other resources that is contemplated is permitted under applicable U.S. law and DOD and Army regulations (see paras I–7 and I–10). Unauthorized expenditure of U.S. government funds may result in violation of the Anti-Deficiency Act, a federal criminal statute.

Question: Is an RVA required for a foreign national who requires access to an Army installation to perform a service under an Army contract?
Answer: No. Visits by foreign nationals who are not representing their governments in an official capacity to Army installations/activities do not require an RVA. However, foreign nationals must meet Army installation access control requirements as delineated in AR 190–13 (see para 1–5g).

Question: Can U.S. contractors serve as FDOs?
Answer: No. Foreign disclosure is an inherently governmental function and must be performed by a DA member (see para 2–11).

Question: What does the command do if a FLO does not sign the certification statement form?
Answer: The contact officer will sign their portion of the certification statement, annotate on the form that the FLO refused to sign the statement, provide a copy of the statement to the FLO, and notify the DCS, G–2 (see para J–2c(3)).

Question: Can a FLO be simultaneously certified to more than one organization?
Answer: No. Certification of a FLO to more than one command or agency is not authorized (see para J–2c(1)).

Question: When is an RVA required for a FLO to visit Army or DOD commands or agencies?
Answer: When the visit is to a destination outside the FLO's terms of certification (see para J–6a(2)).

Question: In exchange programs, a participant may require access to Army computer systems. Which AR controls the granting of this access to Army computer systems for the participant who is working for the Army?
Answer: AR 25–2.

Question: Can FLOs conduct informal coordination for visits prior to an RVA being submitted by their embassy?
Answer: Yes, but with limitations (see para I–3b).

Table F–1.
Frequently asked questions—Continued

Question: Are the dependents of extended visitors authorized dependent ID cards and access to U.S. Government recreational and medical facilities? If so, how is this accomplished?
Answer: Dependents of extended visitors are only allowed ID cards and access to such facilities only if and to the extent authorized by the specific FLO MOU and/or MOA for the extended visitor's country of origin. Dependents of extended visitors are identified by the country's military attaché in the embassy remarks section of the RVA. Additionally, dependents of extended visitors are subject to Army Installation access control requirements as delineated in AR 190–13 (see para I–11c).

Question: Can foreign military personnel visiting Army organizations, activities, and installations on official business wear appropriate civilian attire as opposed to their country's prescribed military uniform?
Answer: Yes, but only when relieved of the responsibility to wear their respective country's uniform by an appropriate DA authority (see para I–8).

Question: Can an ENDP be used to establish a PEP position?
Answer: No. Current DOD policy does not allow ENDPs to be used to establish any extended visitor positions (see para 2–5d).

Question: When is it appropriate to non-sponsor a visit?
Answer: "The recommendation and position to "non-sponsor a visit" is appropriate when the visit is to a commercial or contactor facility and the Army has no interest in the visit. It is not appropriate to non-sponsor a visit to an Army facility, activity, or installation since at a minimum, the Army always has an interest in access and security issues to Army facilities (see para I–12c(3)(c)4).

Question: Who may approve foreign representative attendance at unclassified meetings open to the general public?
Answer: Commanders or agency heads may exercise their delegated visit authority to approve foreign representative visits of this type (see para G–5a(1)).

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 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, 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 and those that are not acquisition-related.

Section II
Acquisition-Related Meetings

G–3. Multinational force compatibility
MFC considerations and bilateral agreements promoting industrial cooperation have resulted in DA's adoption of policies (see 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 70–1.

(3) Meetings convened in cooperation with private, industrial-related associations (for example, Association of the 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 authorized delegated disclosure level for classified material in each NDP–1 category that may be involved. It is essential to remember that RFIs and 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 nonacquisition-related meetings involving only unclassified information does not require prior approval of DCS, 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

a. 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.

b. All proposed international activities must be evaluated for the potential disclosure of CMI. This includes an evaluation of CMI that may be discerned through foreign use and/or testing of Army systems.

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 and/or 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 or the 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 letters of offer and acceptance (LOAs) 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 ASA (ALT); DCS, G–3/5/7; and DCS, 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 Army capability briefing.

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

(1) Provided all NDP–1 conditions have been satisfied and prior to formal acceptance of the LOA by the foreign recipient, disclosure is usually limited to the confidential level. This information may include P&A data, information on general system characteristics and capabilities, and system-related training information necessary to successful operation and maintenance. Specific information on system countermeasures susceptibilities or vulnerabilities or 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 judgment 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 (NDP–1 Category 4) is prohibited without the approval of the DCS, G–2 or their designee and the NDPC.

(3) Any proposed disclosure program must be examined in its entirety in order to determine if any aspects of the proposed program might result in the disclosure of classified information. In the case of proposed security assistance programs, the review must include not only hardware, software, documents (necessary for operation, maintenance, employment, and training), but classified vulnerability data that may be discerned through the operation and testing of the end-item.

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 direct commercial sales (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). ASA (ALT) is the HQDA proponent responsible for the review of licenses for the export of defense articles and services, and the Office of the Deputy Secretary of the Army for Defense Exports and Cooperation (ODASA (DE&C)) is the lead 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 12–1.

(1) In coordination with ASA (ALT), DCS, G–2 or their 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 Army weapon system—the PM for that weapon system, with assistance from the supporting FDO, will be responsible for overseeing the DCS cases involving their system and ensuring U.S. contractor compliance with current Army and USG export and disclosure policy provisions. The PM will report any conflict with established export policies to ASA (ALT); DCS, G–3/5/7; DCS, 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 paragraph H–6*a*(2), such as the transfer of single classified military items for test and evaluation under foreign security control, may be authorized only when all of the following conditions are satisfied:

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

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

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

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

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

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

c. Proposals to authorize foreign test and evaluation in this manner will be submitted to ASA (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 ASA (ALT); DCS, 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 DCS, G–2 a copy of the proposal. DCS, 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 paragraphs H–6*b*(1) through H–6*b*(3).

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 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 and/or 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 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. 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 in accordance with paragraph H–7*a*. 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 American, British, Canadian, Australian, and New Zealand Armies (ABCA) MFC (see AR 34–1).

(2) International cooperative R&D programs (see AR 70–41).

(3) The Technical Cooperation Program (see 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 (see AR 70–41) and MPEP (see 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 their designee. In those cases where the Army participates as an establishment under the authority of another Service's international agreement, a supporting Army DDL must be approved by the appropriate Army disclosure authority.

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. The disclosure of system-specific developmental CMI under other types of R&D cooperative agreements (such as DEAs or information exchange annexes (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 their 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 their 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 their 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 and CUI 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. The DA International Visits Program is managed through the Foreign Visits System on the SIPRNET.

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 and CUI authorized for disclosure to their respective governments by a disclosure official designated according to this regulation. CMI and CUI 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
a. The fact that a proposed visit begins by informal coordination does not eliminate the need for an official RVA. 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 formally request visits by their country's officials. These proposals and requests become official only upon the submission of an RVA to DCS, 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 DCS, G–2.

b. FLOs who are interested in informally coordinating a proposed visit must consult with their contact officer for advice on how to proceed.

(1) If the proposed visit involves only the FLO and falls within the FLO's terms of certification, the visit may be coordinated through foreign disclosure channels.

(2) If the proposed visit involves foreign visitors, other than the FLO, to a Army command with a certified FLO from the same foreign country, the FLO may conduct the informal coordination necessary for the visit through foreign disclosure channels. At the conclusion of informal coordination, submission of a formal RVA by the foreign military attaché or designated foreign attaché staff personnel is required.

(3) All informal coordination of a visit outside the FLO's terms of certification must be conducted by the foreign military attaché or designated foreign attaché staff personnel.

I–4. Classified military information and controlled unclassified information documentary transfers
For detailed information on documentary requests for U.S. CMI and CUI, see paragraph 3–5.

I–5. Foreign Visits System requirements
a. All Army FDOs, alternate FDOs, and personnel who process RVAs are required to have a SPAN account and access to the SIPRNET.

b. An accredited military attaché or designee using the FVS will submit foreign government RVAs. Requests for visits by governments that do not utilize the FVS will be submitted by the accredited military attaché, in writing, directly to DCS, G–2, which will enter the request in the FVS and process it through the FVS.

I–6. Visit requests from countries and international organizations without a military attaché
a. If a foreign government does not have a military attaché diplomatically accredited to the U.S., an embassy official of that government or the senior U.S. military representative located in the prospective visitors' parent country may prepare and submit the RVA to DCS, G–2 for consideration. The RVA must conform to the policies and procedures for submission of RVAs in this regulation and DODD 5230.20.

b. RVAs from international organizations may be submitted by the appropriate international organization security office via letter, email, fax, or in person to the DCS, 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 government 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 must still 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 formal invitation, DA officials will inform the appropriate FDO of the proposed issuance of the invitation and the extent of any anticipated disclosure of CMI or CUI to ensure compliance with this regulation. The requirement to submit an RVA for personnel traveling on ITOs does not apply to foreign personnel who are traveling for training purposes (see para 1–5*g*).

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 or CUI 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 relieved of this responsibility by an appropriate DA authority. When this policy exemption is exercised, it will present a benefit to the U.S. Government and potential risks will be mitigated by sound local security practices and procedures. 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 DCS, G–2 for action. See paragraph 1–5*g* 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 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 one 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 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 para I–11c) and therefore will require the submission of a separate request for extended visit authorization for this particular visit.

c. 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.

(3) If the extended visitor will be accompanied by dependents, the foreign military attaché will use the Embassy Remarks section of the Extended Visit Request to provide the following dependent identifying information:

(a) The full name of each accompanying dependent;

(b) The passport number of each accompanying dependent;

(c) The birth date of each accompanying dependent;

(d) The gender of each accompanying dependent;

(e) The country of citizenship of each accompanying dependent; and,

(f) The relationship of each accompanying dependent to the sponsor.

(4) If no dependents are accompanying the extended visitor, a statement to that effect will be entered into the Embassy Remarks section.

d. Submission of self-invited RVAs. In all of the above self-invited visits, approval by DCS, G–2 or their 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 exceptions to the 30-day rule involve the Army National Training Center, which requires RVAs 45 days in advance of the proposed visit date, and EVAs for certification of foreign representatives, which require RVAs 90 days in advance of the proposed visit date. These requirements are outlined in the Military Attaché Guide – Administrative Guidance issued by DCS, G–2 to each embassy that has a military attaché accredited to the 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 DCS, 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 official approval will not be permitted to proceed. In those instances, the Army command or agency will immediately report the incident to DCS, 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 DCS, 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 to the appropriate Army addressees on the following basis:

(a) HQDA, DCS, G–2 will, with few exceptions, only assign RVAs for action to HQDA-level organizations, ACOMs, ASCCs, DRUs, and PEOs exercising jurisdiction over the information, organization, or activity to be visited. Subsequent staffing of visits to subordinate units, activities, and/or organizations or related contractor facilities having an interest in the subject matter of the visit is the responsibility of the requisite ACOM, ASCC, DRU, PM or PEO.

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

(c) Staffing of RVAs by DCS, 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 may 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 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 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 Army would be served in approving the visit.

Note. Should the RVA action addressee or prospective host desire political and/or military advice regarding the requested visit, the organization should contact DCS, G–3/5/7.

(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 or CUI. Instead, each potential disclosure of CMI or CUI 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 and in the best interests of the Army?" If not, the action addressee or prospective host must recommend either denial or hosting the visit at the unclassified level with an annotation in the remarks section that the visit will be at the public domain 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 or CUI?

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

1. CMI or CUI 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 their 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 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. CUI that is not within the authority of a DDL requires approval by the originator of, or the proponent for, that CUI.

4. 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 disclosure of Army information. These visits will involve the disclosure of 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.

5. Non-sponsorship of a visit is appropriate when the visit is to a commercial or contactor facility and the Army has no interest in the visit. It is not appropriate to non-sponsor a visit to an Army facility, activity, or installation due solely to supposed lack of Army interest since, at a minimum, the Army would always have an interest in any associated access and security issues.

d. Army command recommendation. The ACOM, ASCC, or DRU will recommend to DCS, 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 visit POC; DDL number; international or functional agreement; advance coordination instructions for recurring RVAs; and so on).

Note. A visit POC is a DA member who oversees one-time and recurring visits by foreign government representatives to DA components and subordinate organizations. Visit POC responsibilities are outlined in appendix O.

(b) Denial of the visit request if it is determined the subject matter proposed for discussion 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 visit POC; 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.

e. Army decision. Upon receipt of the recommendation of approval, denial, or nonsponsorship, the DCS, G–2 or their 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 and affected Army elements of the decision.

(a) Issue any instructions, limitations, and so on, as well as the name and commercial duty telephone number of the Army visit POC.

(b) Notify requesting military attaché that they 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 DCS, 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 the contractor facility of the decision. A copy of the visit request will accompany the non-sponsorship notice. A non-sponsorship notice does not preclude the visit, provided the contractor has, or obtains, an export license for the export controlled information involved. It is the responsibility of the contractor to consult applicable export regulations to determine licensing requirements regarding the disclosure of export controlled information during such visits by foreign representatives and nationals.

I–13. Amendments

a. Amendments may only accomplish the following:

(1) Add or delete visitors.

(2) Change originally requested date(s) to later date(s).

(3) Cancel a previously submitted RVA whether pending or approved.

b. For instances other than a cancellation, the foreign attaché must contact the designated visit POC of the hosting activity to seek approval for the proposed change prior to submitting the amendment in FVS. If the visit POC concurs with the proposed modifications to the approved RVA, the attaché may submit the amendment.

I–14. Letter of special accreditation

A letter of special accreditation is a document that is issued by the Director of Foreign Liaison, DCS, G–2 and accredits a foreign military attaché to conduct official direct contact with the 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, DCS, G–2 or the Public Affairs Office). The Director of Foreign Liaison, DCS, G–2 will provide copies of the Letters of Special Accreditation to the DA commands or agencies cited in the documents.

I–15. Foreign visitor misconduct

For the purpose of this regulation, misconduct or alleged misconduct on the part of foreign visitors is categorized as either personal misconduct or official misconduct. This distinction is necessary in order to facilitate appropriate reporting actions by DA personnel.

a. Personal Misconduct. Events or actions seen as inappropriate and/or improper that are specific to the personal behavior of the visitor. This includes but is not limited to failure to honor personal debts and financial obligations, disrespectful or unprofessional behavior or conduct with regard to race, creed, gender, religion, or national and/or ethnic heritages. Allegations of personal misconduct will be documented at the local level and referred to the appropriate DA level program manager.

b. Official Misconduct. Events or actions seen as inappropriate or improper that are related to the purpose of the visitors presence at an Army activity, command, organization, or DOD contractor facility. Official misconduct refers to the misuse, abuse of, or violations of permissions, authorities, access, and procedural guidelines governed in Terms of Certification, Delegation of Disclosure Authority Letters, and/or Requests for Visit Authorizations. The following instances of misconduct will be reported in accordance with the provisions of AR 381–12 with an information copy to DCS, G–2:

(1) Exhibits excessive knowledge of or undue interest in DA personnel or their duties which is beyond the normal scope of friendly conversation and the purpose of the foreign visitors official presence;

(2) Exhibits undue interest in the research and development of military technology, military weapons and intelligence systems, or scientific information and is beyond the normal purpose of the foreign visitors official presence;

(3) Attempts to obtain classified or unclassified information beyond the normal purpose of the foreign visitors official presence;

(4) Acquires unauthorized access to classified or controlled unclassified information;

(5) Attempts to place DA personnel under obligation through special treatment, favors, gifts, money, or other means; or,

(6) Attempts to establish business relationships that are outside of normal official duties.

c. All other instances of alleged misconduct will be reported to DCS, G–2.

Appendix J
Foreign Liaison Officers

J–1. Concept

The Army FLO program was established to facilitate cooperation and mutual understanding between the Army and the armies of allied and friendly nations. A FLO is a foreign government military member or civilian employee who is authorized by their 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 FLO also includes foreign representatives who are assigned to Army commands or activities under ITOs to perform specific administrative oversight functions regarding students of their respective governments. These types of representatives are commonly referred to as Country Liaison Officers. There will not be any disclosure of CMI to CLOs. Certification forms and DDLs are required for these foreign representatives. Even though CLOs normally travel on ITOs, RVAs are required as outlined in paragraph I–7a.

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 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 appendix 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 DDL for these individuals. See paragraph J–2*c*(3) for additional information.

c. National representative. A foreign government representative who is assigned to their 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 Army), to conduct liaison activities with DOD and DA. Certification forms and DDLs are required for these foreign representatives. When a foreign national representative desires to visit a DA command or agency or a DA contractor facility, they may submit a one-time or recurring visit request to DCS, 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 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 Army, this requirement is satisfied by an umbrella-type international agreement that is negotiated and concluded on behalf of DA by DCS, G–2.

b. Letter of offer and acceptance. According to DODD 5230.20, when FLOs are physically assigned to Army installations in a security assistance capacity, an LOA is negotiated and concluded on behalf of DA by ASA (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 their 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 with copies to the servicing FDO, the affected ACOM, ASCC, and/or DRU FDO and DCS, G–2. If a FLO declines to sign the certification statement, the contact officer will sign their 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 DCS, 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 Army. These requests can originate directly from the foreign embassy or through the provisions of an LOA. DCS, G–2 or their designee or the U.S. Army Security Assistance Command, if the request is initiated through an LOA, 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 DCS, 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. DDLs are required for all FLO positions regardless of the classification access level required for the position. All FLO DDLs, regardless of the classification access level, are approved by DCS, G–2.

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 Army.

(c) Step 3. DCS, G–2 will coordinate the proposal within HQDA.

(d) Step 4. After HQDA coordination is completed, DCS, G–2 will finalize the decision on the proposal and formally notify the appropriate foreign government embassy. Upon notification of approval by the DCS, G–2, 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 will review the document. Upon approval of the DDL, DCS, G–2 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. Additionally, the appropriate foreign military attaché must provide a photograph and biography of the FLO nominee to the Army FLO program manager before the EVA will be approved.

(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 to proceed. Such proposals will be conveyed in writing through command or agency channels to DCS, 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. DDLs are required for all FLO positions regardless of the classification access level required for the position. All FLO DDLs, regardless of the classification access level, are approved by DCS, G–2.

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 Army.

(c) Step 3. DCS, G–2 will coordinate the proposal within HQDA.

(d) Step 4. After HQDA coordination is completed, DCS, G–2 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 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 will review the document. Upon approval of the DDL, DCS, G–2 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.

b. Processing of foreign liaison officer nominations. If the FLO position is established, DCS, G–2 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 90 days prior to the requested date of arrival and/or assignment of the FLO. In the EVA request, the foreign military attaché provides written notification to DCS, 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.

(g) The FLO will obtain the appropriate U.S. Visa in their passport for themselves and for any accompanying dependents.

(h) In the Embassy Remarks section of the Extended Visit Request, identify any dependents accompanying the FLO, if any. Dependent information must include accompanying family member's full name, passport number, gender, birth date, country of citizenship, and relationship to the sponsor. If no dependents are accompanying the extended visitor, a statement to that effect should be entered into the Embassy Remarks section.

(2) *Step 2*. DCS, G–2 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 the required suspense assigned to the EVA request. See appendix D for detailed information on DDLs.

(3) *Step 3*. Upon receipt of the concurrence of the recipient DA command or agency and receipt of the required photograph and biography from the foreign military attaché, DCS, G–2 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 their duties. The DA command or agency FDO must be notified immediately. The DA command or agency FDO will then notify the DCS, 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 paragraph J–3*a* 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.

J–4. Revalidation of foreign liaison officer positions

a. Annual revalidation. All FLO positions will be revalidated annually to ensure the best interests of the DA and host command or agency continue to be served and the purpose of the position remains valid. ACOMs, ASCCs, and DRUs will provide a consolidated report, in memo form, to DCS, G–2 annually. Guidance and suspense for the revalidation will be issued by DCS, G–2. Reports will provide the following:

(1) The benefit gained by the Army from each FLO position.

(2) The FLO's compliance with the country specific Liaison Officer MOU and/or memorandum of agreement (MOA).

(3) The FLO's compliance with the DDL established for the FLO position.

b. Modification or termination of FLO positions. Recommendations for the modification or termination of a FLO position will be made in writing by the hosting commander, forwarded through the appropriate ACOM, ASCC, or DRU to DCS, G–2. Termination recommendations require a clear justification and flag level signature.

J–5. 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 or 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 other activities, such as airborne operations, piloting 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 their designee. Questions concerning the authorized activities of FLOs will be referred, through command or agency channels, to DCS, G–2 for resolution.

c. FLOs will not represent their governments as associate technical project officers (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 is granted. They may have access to U.S. CMI authorized for disclosure to their government as defined in the position DDL and 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. Email addresses will be in accordance with AR 25–2.

i. While assigned to a DA and/or 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–6. 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 DCS, G–2.

(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 their 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 25–2 and local security procedures will apply.

d. Misconduct. When assigned to the 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 (see para I–15). Any instances of personal misconduct will be reported to DCS, G–2, in a timely manner, with details of corrective action taken or a recommendation for final disposition by HQDA, such as temporary suspension or permanent revocation of privileges, or revocation of certification. DCS, G–2 will coordinate the resolution of all cases involving FLO personal misconduct.

J–7. 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 their command or agency.

b. Providing the command position on the RVA in accordance with the assigned suspense.

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

d. Facilitate uploading signed terms of certification and the computer usage statement to SENTRY within ten days of the signing date. In those cases where use of SENTRY is not possible, DCS, G–2 will accept a hard copy.

J–8. United States contact officer

The responsibilities outlined in paragraphs O–2 through O–3 of this regulation apply.

J–9. 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 Army activity or installation is not necessary (that is, the FLO office is not located on the Army activity or installation). There are two types of foreign nationals that may be hired by FLOs as administrative support personnel: individuals in the U.S. 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 DCS, G–2 of the hiring if access (ingress and egress) to the installation is required. For foreign disclosure purposes, these administrative personnel are considered to be foreign representatives.

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 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 Army facilities in the company of the FLO.

f. Army activities will develop positional ingress and/or egress DDLs for each administrative support position. Electronic copies of the positional ingress and/or egress DDLs will be forwarded to DCS, G–2 within ten working days of approval.

(Office Symbol) (Date)

SECTION I
LIAISON OFFICER
LEGAL STATUS OF CERTIFICATION

As a representative of the (foreign government/international organization) under the auspices of foreign military sales (FMS) case number (FMS case number) 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.

SECTION II
LIAISON OFFICER
CONDITIONS OF CERTIFICATION

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 (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 non-duty hours, I am required

Figure J–1. Certification for Security Assistance Foreign Liaison Officers

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 non-duty access.

8. Security.

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

f. I understand that I may take custody of U.S. Government (enter classification level) information to perform courier functions when authorized by my parent government. Such authorization will be in writing.

g. I understand that all U.S. classified material 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.

h. I may not reproduce U.S. 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. 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.

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

Figure J–1. Certification for Security Assistance Foreign Liaison Officers—Continued

SECTION III
LIAISON OFFICER
CERTIFICATION OF IN-BRIEFING

I, (name of liaison officer), understand and acknowledge that I have been certified as a security assistance liaison officer to (place), as agreed upon between (name of country) and the U.S. Army. I further acknowledge that I fully understand and have been briefed on the legal status and conditions of my certification. I further acknowledge that I will comply with the conditions and responsibilities of my certification.

_____ _____
(SIGNATURE OF LIAISON OFFICER) (SIGNATURE OF BRIEFER)

_____ _____
(TYPED NAME OF LIAISON OFFICER) (TYPED NAME OF BRIEFER)

_____
(RANK AND/OR TITLE)

_____
(DATE)

Figure J–1. Certification 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 which I may have been granted. I understand that my acceptance of the liaison officer position does not bestow diplomatic or other special privileges.

SECTION II
LIAISON OFFICER
CONDITIONS OF CERTIFICATION

1. Responsibilities. I understand that my activities will be limited to the representational responsibilities of my government and that I am expected to present the views of my government with regard to the issues 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, which 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

Figure J–2. Sample Certification for Operational Foreign Liaison Officers

Department of Defense facilities, unless otherwise directed. I will comply with my parent government's service uniform regulations.

7. Duty Hours. I understand that my duty hours are Monday through Friday, from (time) to (time). Should I require access to my work area during non-duty hours, I am required to request permission from the command security officer. I further understand that (it is)(it is not) necessary to assign a U.S. escort officer to me during my non-duty access. Any cost incurred as a result of such non-duty access may be reimbursable to the 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 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. Citizenship and Immigration Services.

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

Figure J–2. Sample Certification for Operational Foreign Liaison Officers—Continued

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. (Note. 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 (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 LIAISON OFFICER (SIGNATURE OF BRIEFER)

_____ _____

Figure J–2. Sample Certification for Operational Foreign Liaison Officers—Continued

(TYPED NAME OF LIAISON OFFICER) (TYPED NAME OF BRIEFER)

_____
(RANK AND/OR TITLE)

_____
(DATE)

Figure J–2. Sample Certification for Operational Foreign Liaison Officers—Continued

(Office Symbol) (Date)

SECTION I
LIAISON OFFICER
LEGAL STATUS OF CERTIFICATION

As a representative of (name of country) under the auspices of an extended visit authorization to the 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 which I may have been granted. I understand that my acceptance of the liaison officer position does not bestow diplomatic or other special privileges.

SECTION II
LIAISON OFFICER
CONDITIONS OF CERTIFICATION

1. Responsibilities. I understand that my activities will be limited to the representational responsibilities of my government and that I am expected to present the views of my government with regard to the issues 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 my certification. I also understand that requests for information, which are beyond the terms of my certification, will be made through the Office of the Defense Attaché.

5. Other Visits. I understand that authorization for 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 when conducting business at the (location of the U.S. government facility) or other Department of Defense facilities,

Figure J–3. Sample Certification for Specific Operational Foreign Liaison Officers

unless otherwise directed. I will comply with my parent government's service uniform regulations.

7. Duty Hours. I understand that my duty hours are Monday through Friday, from (time) to (time). Should I require access to my work area during non-duty hours, I am required to request permission from my contact officer, who will provide the proper authorizations from the command security officer.

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 their 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 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. Citizenship and Immigration Services.

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 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 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. Arrangements for the storage of parent participant classified information must be accomplished in advance and in writing. The approved procedures will require the material arrives through government-to-government channels and the foreign government provides receipt for the material.
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.

Figure J–3. Sample Certification for Specific Operational Foreign Liaison Officers—Continued

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

f. I will immediately report to 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 and Alternate Contact Officer. (Insert name of contact officer and alternate contact officer) have been assigned as my contact officer and alternate contact officer.

2. Certification. I am certified to the U.S. Army in support of the following programs, topics, and so on. (Note. Paragraph 5 of the DDL may be used as the basis to develop this section)

a. Operational liaison duties.

b. Standardization representative duties. As an operational liaison officer to (name of location), I also have additional responsibilities as a standardization representative under the auspice of the ABCA Standardization Program. When visiting U.S. Army installations to attend ABCA conferences or meetings or to conduct ABCA specific business at that site, I will not be required to have an embassy initiated visit authorization. Clearance certification and access to information will be provided directly from the parent ABCA organization to the meeting host, ODCS, G-3/5/7, 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).

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

Figure J–3. Sample Certification for Specific Operational Foreign Liaison Officers—Continued

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 U.S. Army (organization) as approved by the (name of country) 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 LIAISON OFFICER (SIGNATURE OF BRIEFER)

_____ _____
(TYPED NAME OF LIAISON OFFICER) (TYPED NAME OF BRIEFER)

_____
(RANK AND/OR TITLE)

_____
(DATE)

Figure J–3. Sample Certification 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

Figure J–4. Foreign Liaison Officer Letter of Offer and Acceptance Conditions & Limitations

for the particular unit of the Host Party, which the Liaison Officer is serving. The Liaison Officer will comply with the customs of the Host Party with respect to the wear of civilian clothing.

9. Prior to the commencement of a Liaison Officer's tour, the Parent Party will notify the Host Party of the specific Parent Party organization which will exercise operational control over the Liaison Officer and, if different, the Parent Party organization that will provide administrative support to the Liaison Officer and the Liaison Officer's dependents.

10. At the end of a Liaison Officer's tour, or as otherwise agreed by the Parties, the Parent Party may replace the Liaison Officer with another individual who meets the requirements of this LOA. Such replacement will be subject to any certification or approval requirements imposed under the laws and regulations of the Host Party.

11. The Host Party's certification or approval of an individual as a Liaison Officer will not, in and of itself, bestow diplomatic or other special privileges on that individual.

12. The Host Party will establish the maximum substantive scope and classification levels within which the disclosure of any classified information or controlled unclassified information to the Liaison Officer will be permitted. The Host Party will inform the Parent Party of the level of security clearance required to permit the Liaison Officer access to such information.

13. Each party will cause security assurances to be filed stating the security clearances for the Liaison Officer being assigned by such party. The security assurances will be prepared and forwarded through prescribed channels in compliance with established Host Party procedures.

14. The Parent Party will ensure that each assigned Liaison Officer is fully cognizant of, and complies with, applicable laws and regulations concerning the protection of proprietary information (such as patents, copyrights, know-how, and trade secrets), classified information and controlled unclassified information disclosed to the Liaison Officer. This obligation will apply both during and after termination of an assignment as a Liaison Officer. Prior to taking up duties as a Liaison Officer, the Liaison Officer will be required to sign the certification form. Only individuals who execute the certification form will be permitted to serve as Liaison Officers.

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.

Figure J–4. Foreign Liaison Officer Letter of Offer and Acceptance Conditions & Limitations—Continued

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/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.

Figure J–4. Foreign Liaison Officer Letter of Offer and Acceptance Conditions & Limitations—Continued

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 & Limitations—Continued

Appendix K
Standardization Representatives

K–1. Concept

a. The ABCA Armies 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 Armies Program has produced more than 1,000 standardization agreements, known as ABCA Standards, to advance interoperability between the five nations especially in coalition operations. The current ABCA Armies 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–3/5/7 is the DA proponent for this program, and AR 34–1 is the proponent regulation.

b. Under the authority of the BSA, each of the armies participating in the ABCA Armies 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, Australian or New Zealand StanReps in the U.S. are certified as operational FLOs, who perform the StanRep function as additional duties.

c. ABCA Capability Groups are the basic forums used to exchange information and work on improving the capability of ABCA armies to operate together in a coalition environment. ABCA Support Groups provide advice and support to the Program, especially to the Capability Groups, in relation to their support area. There are five Capability Groups, three Support Groups and NPOCs represented in each group.

d. Capability Groups develop topics for inclusion on a standardization list (StanList), which is available online (http://www.abca-armies.org). 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 Army will assume responsibility, the U.S. NPOC will ensure the normal foreign disclosure approval process as cited in this regulation is affected.

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 paragraphs J–5 and J–6*d* of this regulation apply for StanReps.

K–5. Administering standardization representatives

The procedures outlined in paragraph J–6 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 Army representatives or not approved by the ABCA Armies Program.

K–6. Foreign disclosure officer

The responsibilities outlined in paragraph J–7 of this regulation apply. Additionally, in the event that a BCA StanRep requests 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 Capability Group for that particular topic. The list of the Capability Groups and associated NPOCs for each Capability Group is available online (http://www.abca-armies.org).

K–7. United States contact officer

The responsibilities outlined in paragraphs O–2 through O–3 of this regulation apply.

(Office Symbol) (Date)

SECTION I
LIAISON OFFICER
LEGAL STATUS OF CERTIFICATION

As a representative of (name of country) under the auspices of an extended visit authorization to the 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 which I may have been granted. I understand that my acceptance of the liaison officer position does not bestow diplomatic or other special privileges.

SECTION II
LIAISON OFFICER
CONDITIONS OF CERTIFICATION

1. Responsibilities. I understand that my activities will be limited to the representational responsibilities of my government and that I am expected to present the views of my government with regard to the issues 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. Standardization Representative Duties. As a liaison officer certified to (name of location), I also have additional 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 or to conduct ABCA specific business at that site, I will not be required to have an embassy initiated visit authorization but will provide my contact officer with 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 the 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 is available on the ABCA Web site and any issues with those 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.

Figure K–1. Sample Certification for StanRep

5. 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 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, which are beyond the terms of my certification, will be made through the Office of the Defense Attaché.

6. Other visits. I understand that authorization for 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 non-duty hours, I am required to request permission from the command security officer. I further understand that (it is)(it is not) necessary to assign a 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 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.
b. I understand that my administrative support person will not be permitted to act on my behalf or represent my government.
c. I understand that any security clearance associated with my administrative support person will be sponsored and issued by my parent government.
d. I understand that my administrative support person, if a foreign national, will have the appropriate status to work in the U.S. This work status is defined by the Department of State in conjunction with the U.S. Citizenship and Immigration Services.

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 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 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

Figure K–1. Sample Certification for StanRep—Continued

disclosed by me to any other person, firm, organization, or government without the prior written authorization of the 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. Arrangements for the storage of parent participant classified information must be accomplished in advance and in writing. The approved procedures will require the material arrives through government-to-government channels and the foreign government provides receipt for the material.

d. While assigned to (Army Organization), I will comply with all 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 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. (Insert name of contact officer) have 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. (Note. Paragraph 5 of the DDL maybe 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).

Figure K–1. Sample Certification for StanRep—Continued

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 (name of country) and the U.S. (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 LIAISON OFFICER)

_____ (SIGNATURE OF BRIEFER)

_____ (TYPED NAME OF LIAISON OFFICER)

_____ (TYPED NAME OF BRIEFER)

_____ (RANK AND/OR TITLE)

_____ (DATE)

Figure K–1. Sample Certification for StanRep—Continued

Appendix L
Military Personnel Exchange Program

L–1. Concept

The Military Personnel Exchange Program with Armies of Other Nations involves the assignment of Army and foreign armed forces personnel to authorized positions within each party's military establishment. The DCS, G–3/5/7 is the proponent for the program and directs it under the provisions of AR 614–10. MPEP is an Army security cooperation program. In accordance with applicable exchange program regulations, foreign military personnel are integrated into the DA work force. Such exchanges are established under a formal MOA between the Army and a foreign military service under AR 550–51.

L–2. Conditions and limitations

a. MPEP participants will not act in the dual capacity as a foreign exchange personnel participant and as a representative of their government (for example, a FLO) while assigned to a DA command.

b. MPEP participants will not serve as conduits between DA and their government for requests and transmission of CMI and CUI nor be used as a mechanism for exchanging technical data or other controlled information between the governments.

c. MPEP participants will not be assigned to command or other positions that would require them to exercise responsibilities reserved by law or regulation to an officer or employee of the USG. They will not, for example,

perform responsibilities of a contracting officer's technical representative, component duty officer, classified document custodian or security officer, escort for foreign visitors, or perform other official acts as a representative of DA.

d. MPEP participants will not be assigned to DOD contractor facilities.

e. DA will not submit ENDP requests solely to accommodate the establishment of a MPEP position.

f. The assignment of MPEP participants will not be used for training foreign personnel in violation of DOD 5105. 38–M or, instead of, or in combination with MPEP certification. Pursuant to Section 1082 of Public Law 104–201, training may not be conducted under the MPEP except as necessary to familiarize, orient, or certify MPEP participants regarding unique aspects of the positions to which they are assigned.

g. MPEP participants will not be placed in duty positions that could result in their access to CMI or CUI that has not been authorized for disclosure to their government.

h. MPEP participants will not have permanent (documentary) custody of CMI and CUI. They may have access to the information during normal duty hours at the place of assignment when access is necessary to perform their duties and the information is authorized for disclosure pursuant to the supporting DDL. As such, documentary disclosures are not appropriate for inclusion in DDLs for MPEPs.

i. MPEP participants' access to restricted areas will be in accordance with AR 190–13 and local security policies and procedures and as specified in the supporting DDL.

j. MPEP participants will wear their uniforms in accordance with local command customs and tradition. If required, they will wear, in clear view, a DA building or installation pass or badge that clearly identifies them as foreign nationals.

k. Any other identification (including organizational code and title, block, office nameplate, security badge, or email address) used by or issued to MPEP participants by the host Army units will clearly identify the MPEP participant's status as a foreign national. Email addresses will be in accordance with AR 25–2.

L–3. Military Personnel Exchange Program memorandum of agreement and certification

a. MOA. AR 614–10 provides detailed information on MPEP MOAs.

b. Certification.

(1) MPEP participants are certified to DA commands or agencies to perform assigned duties. Terms of certification are derived from and are consistent with the scope of the MOA.

(2) Each MPEP participant must sign a certification statement acknowledging the terms of their assignment. A copy of the signed certification statement, which will be maintained by the local FDO, must be provided to the MPEP with copies to the servicing FDO, ACOM, ASC, and/or DRU FDO, DCS, G–2 and DCS, G–3/5/7, HQDA. If the MPEP participant refuses to sign the certification statement, the command or agency must immediately notify the DCS, G–3/5/7, HQDA program manager who will resolve the issue through the parent government's military attaché in Washington, DC.

L–4. Establishment of Military Personnel Exchange Program positions and processing of Military Personnel Exchange Program nominations

a. Establishment of MPEP positions. Only the HQDA proponent may approve establishment, disestablishment, or changes to MPEP positions. A DDL is required for all MPEP positions and must be approved prior to finalizing the establishment of the position.

b. Processing of visit requests for MPEP nominations. All visit requests for MPEP nominations will be processed in the following manner:

(1) Step 1: The appropriate foreign military attaché will submit an RVA at least 90 days prior to the requested date of assignment of the MPEP participant. In the RVA request, the foreign military attaché provides written notification to DCS, G–2, HQDA of the following:

(a) Subject individual is an officially-sponsored exchange participant of that government.

(b) The official holds the specified level of security clearance.

(c) The parent government will assume the responsibility for any and all U.S. CMI provided to the MPEP participant.

(2) Step 2: DCS, G–2, HQDA will process the RVA to the program manager and command or agency to which the MPEP participant is to be assigned. Since the position DDL outlining the terms of the certification of the MPEP participant will be pre-coordinated and approved, the recipient DA command or agency should respond favorably within the required suspense for the RVA request. See appendix D for detailed information on DDLs.

(3) Step 3: Upon receipt of the concurrence of the recipient command or agency, approval of the supporting DDL, and after obtaining a photograph and biography from the respective embassy, DCS, G–2, HQDA will approve the RVA and notify DCS, G–3/5/7, HQDA, the foreign military attaché, and the recipient command or agency of the approval. The foreign military attaché will then coordinate with the recipient command or agency for the arrival of the MPEP participant.

Note. DA commands or agencies may not accept a MPEP participant until the DDL and visit request have been approved. If an MPEP participant arrives prior to visit approval, the command or agency involved will not permit the MPEP participant to

commence their duties. The command or agency FDO must be notified immediately. The command or agency FDO will then notify DCS, G–2, HQDA, who will coordinate the disposition of MPEP participant with DCS, G–3/5/7, HQDA and the appropriate foreign military attaché and provide instructions to the command or agency FDO.

c. Modification of a MPEP position. Any proposal to change the scope of a MPEP participant's certification will be in accordance with the procedures outlined in AR 614–10, with emphasis on the specific modification. DCS, G–3/5/7, HQDA will effect the necessary coordination (that is, modifications to an existing DDL, if required) to render a decision regarding the request. Any proposal to extend the MPEP participant's duration must be initiated and requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under the "purpose of visit request" section of the extension request, the appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

d. Assessment of MPEP positions. All Army MPEP positions must be routinely assessed to determine if the exchange should continue. Assessment procedures will be in accordance with the procedures outlined in AR 614–10.

L–5. Administering Military Personnel Exchange Program participants

a. Visits. All visits or travel by the MPEP participant will be in accordance with the standing operating procedures of the unit of assignment and AR 614–10. However, all travel orders will identify the individual as a MPEP participant assigned to the Army.

b. Library and Publications Support. At the discretion of the host activity's contact officer and through coordination with the FDO, a MPEP may be granted supervised access to the CMI section of the command or agency library. Additionally, each MPEP may be provided a reference set of DA and activity publications necessary to the successful performance of the MPEP's duties, consistent with the MPEP's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the MPEP's successor when their certification ends.

c. Computer Access. MPEPs may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is authorized for disclosure to their government. In all cases, the provisions of AR 25–2 and local security procedures will apply.

d. Misconduct. MPEPs serve at the pleasure of DA and will comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If a MPEP violates the terms of certification, violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the hosting command will provide a written report regarding the inappropriate action, through proper channels (see para I–15). Those instances of personal misconduct will be reported to DCS, G–3/5/7, HQDA, in a timely manner, with the details of the corrective action taken and a recommendation for final disposition, such as temporary suspension or permanent revocation of privileges, or revocation of certification. DCS, G–3/5/7, HQDA will provide a copy of the report to DCS, G–2, HQDA and coordinate the resolution of all MPEP misconduct cases.

L–6. Foreign disclosure officer

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

a. Assisting in the development of the DDL associated with each MPEP position established within their respective command or agency.

b. Providing a position on the RVA in accordance with the assigned suspense.

c. Providing advice and assistance on all matters pertaining to the disclosure of CMI and CUI to each MPEP assigned to the respective command or agency.

d. Maintaining a copy of the MPEP certification statement (see AR 614–10).

e. Notifying the MPEP Program Manager through command channels of any MPEP misconduct (see AR 614–10).

f. Briefing MPEP Contact Officer on their duties (see AR 614–10).

L–7. Supervisor functions

DA officials designated to supervise a MPEP participant will—

a. Ensure that the MPEP participant understands the duties to be performed in the assigned position.

b. Ensure that the MPEP participant is provided access only to that CMI and CUI necessary to fulfill the duties of the position description as described in the DDL.

c. Be familiar with this regulation, other applicable regulatory guidance governing the disclosure of CUI, and specific disclosure guidelines established in the DDL.

d. Inform co-workers of the disclosure limitations on access to CMI and CUI related to the MPEP participant and their responsibilities in dealing with the MPEP participant.

e. Ensure that the MPEP participant signs a certification before being assigned to the position.

f. Ensure the DDL is not provided to the MPEP participant. The DDL is a U.S. eyes-only document. See paragraph D–5 of this regulation.

L–8. United States contact officer

The responsibilities outlined in paragraphs O–2 and O–4 of this regulation apply.

Appendix M
Engineers and Scientists Exchange Program

M–1. Concept

The ESEP is a professional development endeavor that promotes international cooperation in military research, development, test, and evaluation (RDT&E) through the exchange of military and/or government civilian scientists and engineers. This program provides on-site working assignments for foreign personnel in Army activities, and for U.S. personnel in foreign army activities. The work assignments will provide ESEP personnel work experience as spelled out under an approved position description and at the direction of a host supervisor, as well as knowledge of the organization and management of that army establishment to which they are assigned. Within the Army, the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation (DASA (DE&C)) in the ASA (ALT) is the Army lead agent and exercises Army responsibility for coordinating placement of foreign personnel in Army installations under the provisions of AR 70–41.

a. The goals of the program are to leverage state-of-the-art technology of mutual interest to the U.S. and the foreign country involved, conserve scarce resources by reducing duplicative RDT&E efforts, and promote mutual cadres of defense professionals who will continue to support international armaments cooperation activities.

b. The ESEP is not a training program, a means of exchanging personnel for production or co-development purposes, nor a means of augmenting personnel resources above currently authorized manning levels.

M–2. Conditions and limitations

a. ESEP participants will not act in the dual capacity as a foreign exchange personnel participant and as a representative of their government (for example, a FLO) while assigned to a DA command or agency.

b. ESEP participants will not serve as conduits between DA and their government for requests and transmission of CMI and CUI nor be used as a mechanism for exchanging technical data or other controlled information between the governments.

c. ESEP participants will not be assigned to command or other positions that would require them to exercise responsibilities reserved by law or regulation to an officer or employee of the USG. They will not, for example, perform responsibilities of a contracting officer's technical representative, component duty officer, classified document custodian or security officer, escort for foreign visitors, or perform other official acts as a representative of DA.

d. ESEP participants will not be assigned to DOD contractor facilities.

e. DA will not submit ENDP requests solely to establish an ESEP position.

f. The assignment of ESEP participants will not be used for training foreign personnel in violation of DOD 5105. 38–M or, instead of, in combination with FLO certification. Pursuant to Section 1082 of Public Law 104–201, training may not be conducted under the ESEP except as necessary to familiarize, orient, or certify ESEP participants regarding unique aspects of the positions to which they are assigned.

g. ESEP participants will not be used for the purpose of augmenting DA staff positions or as a means to obtain personnel resources beyond authorized manning levels.

h. ESEP participants will not be placed in duty positions that could result in their access to CMI or CUI that has not been authorized for disclosure to their government.

i. ESEP participants may have temporary custody of CMI and CUI necessary to perform their duties and the information is authorized for disclosure pursuant to the DDL. As such, documentary disclosures are not appropriate for inclusion in DDLs for ESEPs. In all cases, local security policies and procedures apply.

j. ESEP participants' access to restricted areas will be in accordance with AR 190–13 and local security policies and procedures and as specified in DDLs.

k. ESEP military participants will wear their uniforms while civilian participants will wear civilian attire in accordance with local command customs and tradition.

Note. In the event such clothing poses a safety hazard (for example, in a laboratory setting), allowances to this requirement may be made by authorized personnel. They will wear, in clear view, a DA building or installation pass or badge (if required) that clearly identifies them as foreign nationals.

l. Any other identification (including organizational code and title, block, office nameplate, security badge, or email address) used by or issued to ESEP participants by the host Army units will clearly identify the ESEP participant's status as a foreign national. Email addresses will be in accordance with AR 25–2.

m. ESEP participants will sign a statement regarding invention rights.

M–3. Engineers and Scientist Exchange Program memorandum of understanding and certification

a. MOU. AR 70–41 provides the overarching authority for the ESEP.

b. Certification.

(1) ESEP participants are certified to a DA activity to perform duties of their approved position description, Certificate of Conditions and Responsibilities, Commitment Regarding Inventions Made and Technical Information Developed by Visiting Engineers and Scientists per the applicable MOU, AR 70–41, and RVA. These terms of certification are derived from and are consistent with the scope of existing bilateral ESEP international agreements.

(2) Each ESEP participant must sign the aforementioned Certificate of Conditions and Responsibilities acknowledging the terms of their assignment. The ESEP participant will be provided a copy of the signed certification during in-processing. If the ESEP participant refuses to sign the certification statement, the command or agency must immediately notify the Army lead agent, which will notify DCS, G–2, HQDA, and together resolve the issue with the parent government's military attaché in Washington, DC.

M–4. Establishment of Engineers and Scientists Exchange Program positions and processing of Engineers and Scientists Exchange Program nominations

a. Establishment of ESEP positions. Only the Army lead agent may approve the establishment of ESEP assignments. The Army lead agent is responsible for coordinating prospective ESEP positions with the relevant host placement activity level, ACOM level, and DA level entities. A DDL is required for all ESEP positions.

Note. Within HQDA, the Army lead agent, ASA (ALT), will coordinate ESEP actions with the following offices (at a minimum): DCS, G–2 and (as required) the Office of the General Counsel. The following ESEP establishment procedures are as follows:

(1) The Army lead agent will forward the assignment request to the Army host activity, which will examine the nomination to ensure that the nominee is qualified for the proposed position.

(2) The host activity must ensure that the entire ESEP assignment request package (that is, Host Endorsement Letter, Position Description, Professional Background (that is, a Resume), Career Areas of Interest, and DDL) is completed no later than 60 days following receipt of the assignment request.

(3) The Army lead agent, upon receipt of the assignment request package from the host activity, will coordinate the assignment request package and execute internal and HQDA coordination to approve the assignment request.

(4) The Army lead agent upon internal review and approval will sign the Assignment Offer Letter and forward it and the position description to the foreign ESEP lead agent for acceptance. The Certificate of Conditions and Responsibilities and Commitment Regarding Inventions Made and Technical Information Developed will be signed by the participant after reporting for duty at the in-processing session and/or briefing.

(5) Upon receipt of the assignment acceptance from the foreign ESEP lead agent, the Army lead agent will notify the nominee's Embassy to submit the RVA.

b. Processing of ESEP nominations. The procedures for processing ESEP assignment requests can be found in the ESEP MOU, AR 70–41, and the Handbook, chapter 4. In summary, upon receipt of the foreign government nomination:

(1) Step 1: The appropriate foreign military attaché will submit an RVA request at least 45 days prior to the requested date of assignment of the ESEP participant. In the RVA request, the foreign military attaché provides written notification to DCS, G–2, HQDA of the following:

(a) Subject individual is an officially-sponsored exchange participant of that government.

(b) The official holds a specified level of security clearance.

(c) The parent government will assume the responsibility for any and all U.S. CMI provided to the ESEP participant.

(2) Step 2: DCS, G–2, HQDA will process the RVA request to the program manager and command or agency to which the ESEP participant is to be assigned. Since the position DDL outlining the terms of the assignment and/or position description of the ESEP participant will be pre-coordinated and approved, the recipient DA command or agency should respond favorably within the required suspense assigned to the RVA request. The position DDL or equivalent disclosure guidance will remain valid until there is a change to the scope of the position or the position is terminated. See appendix D for detailed information on DDLs.

(3) Step 3: Upon receipt of the concurrence of the recipient program manager and command or agency, approval of the supporting DDL, and after obtaining a photograph and biography from the respective embassy, DCS, G–2, HQDA will approve the RVA request and notify ODASA (DE&C), the Army lead agent, the foreign military attaché, and the recipient command or agency of the approval. The foreign military attaché will then coordinate with the recipient command or agency for the arrival of the ESEP participant.

c. DA commands or agencies may not accept an ESEP participant until the position description, DDL and visit request have been approved. If the ESEP participant arrives prior to visit approval, the command or agency involved will not permit the ESEP participant to commence their duties. The command or agency FDO must be notified immediately. The command or agency FDO will then notify DCS, G–2, HQDA, who will coordinate the disposition of

ESEP participant with the Army lead agent, and the appropriate foreign military attaché and provide instructions to the command or agency FDO.

d. Modification of an ESEP position. Any proposal to change the scope of an ESEP participant's position description will be in accordance with the procedures outlined in paragraph M–4*a*, with emphasis on the specific modification. Any proposal to extend the ESEP participant's duration must be initiated and requested by the supervisor of the host command or agency through the Army lead agent for concurrence by the foreign lead agent, and then formally requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, the appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

M–5. Administering Engineers and Scientists Exchange Program participants

a. Visits. All DA-directed visits or travel by the ESEP participant will be in accordance with the work being performed under the approved position description and DDL. All travel orders will identify the individual as an ESEP participant assigned to the Army host activity.

b. Library and publications support. At the discretion of the host command or activity contact officer and through coordination with the FDO, an ESEP participant may have supervised access to the CMI section of the command or agency library as long as it is within the scope of the approved DDL. Additionally, each ESEP participant may be provided a reference set of DA and/or host activity publications necessary to the successful performance of the ESEP position description, consistent with the ESEP participant's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned when the ESEP participant's assignment ends.

c. Computer access. ESEP participants may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is needed to accomplish the work under their approved position description and is authorized for disclosure to their government. In all cases, the provisions of AR 25–2 and local security procedures will apply.

d. Misconduct. ESEP participants serve at the pleasure of DA and will conform to the Army's customs and traditions and will comply with all applicable statutory and regulatory (DOD, DA, and local) guidance. If an ESEP participant violates the terms of certification, violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the hosting command will provide a written report regarding the inappropriate action, through proper channels (see para I–15). Those instances of personal misconduct will be reported to the Army lead agent, in a timely manner, with the details of the corrective action taken or a recommendation for final disposition, such as temporary suspension or permanent revocation of privileges, or revocation of certification. The Army Agent will provide DCS, G–2, HQDA, with a copy of the report and coordinate the resolution of all ESEP misconduct cases.

M–6. Foreign disclosure officer

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

a. Assisting in the development of the DDL associated with each ESEP position established within their respective command or agency.

b. Providing a position on the RVA request in accordance with the assigned suspense.

c. Providing advice and assistance on all matters pertaining to the disclosure of CMI and CUI to each ESEP position assigned to the respective command or agency.

d. Notifying the ESEP Program Manager through command channels of any ESEP misconduct.

e. Briefing ESEP Contact Officer on their duties.

M–7. Supervisor functions

The ESEP participant's supervisor will—

a. Ensure that the ESEP participant understands the work to be performed under the approved position description.

b. Ensure that the ESEP participant is provided access only to that information necessary to fulfill the duties of the position description as described in the DDL.

c. Inform co-workers of the access limitations related to the ESEP participant and their responsibilities in dealing with the ESEP participant.

d. Ensure that the ESEP participant signs all required documentation (as mentioned above, as well as any local host documentation) before being assigned to the position.

e. Be familiar with this regulation, other applicable regulatory guidance governing the disclosure of CUI, and specific disclosure guidelines established in the DDL.

f. Ensure the DDL is not provided to the ESEP participant. The DDL is a U.S. eyes-only document. See paragraph D–5 of this regulation.

M–8. United States contact officer

The responsibilities outlined in paragraphs O–2 and O–5 of this regulation apply.

Appendix N
Cooperative Program Personnel

N–1. Concept

a. Foreign representatives may be assigned to international program offices that are hosted by a DA Component as part of an international management team responsible for the implementation of a international project or program. Foreign representatives assigned to CPP positions will be military members or civilian employees of the counterpart foreign government defense organization. The Office of the DASA (DE&C) in the ASA (ALT) is the DA proponent for this program which is governed under the provisions of AR 70–41.

b. Only foreign government personnel assigned to an international program office, hosted by an Army command or agency pursuant to the terms of a Cooperative Program and/or Project Annex or Article to an International Cooperative RDT&E and/or Acquisition Agreement, and who report to and take direction from an Army-appointed U.S. PM (or PM-equivalent) will be accorded the treatment described in this appendix.

N–2. Conditions and limitations

a. CPP participants will not act in the dual capacity as a foreign exchange personnel participant and as a representative of their government (for example, a FLO) while assigned to a DA command.

b. CPP participants will not serve as conduits between DA and their government for requests and transmission of CMI and CUI nor be used as a mechanism for exchanging technical data or other controlled information between the governments.

c. CPP participants will not be assigned to command or other positions that would require them to exercise responsibilities reserved by law or regulation to an officer or employee of the USG. They will not, for example, perform responsibilities of a contracting officer's technical representative, duty officer, classified document custodian or security officer, escort for foreign visitors, or perform other official acts as a representative of DA.

d. CPP participants will not be assigned to DOD contractor facilities.

e. The assignment of CPP participants will not be used for training foreign personnel in violation of DOD 5105. 38–M or, instead of, in combination with CPP certification. Pursuant to Section 1082 of Public Law 104–201, training may not be conducted under the CPP except as necessary to familiarize, orient, or certify CPP participants regarding unique aspects of the positions to which they are assigned.

f. CPP participants will not be used for the purpose of augmenting DA staff positions or as a means to obtain personnel resources beyond authorized manning levels.

g. CPP participants will not be placed in duty positions that could result in their access to CMI or CUI that has not been authorized for disclosure to their government.

h. CPP participants will not have permanent custody of CMI and CUI. They may have access to the information during normal duty hours at the place of assignment when access is necessary to perform their duties and the information is authorized for disclosure pursuant to the DDL. In all cases, local security policies and procedures apply.

i. CPP participants' access to restricted areas will be in accordance with AR 190–13 and local security policies and procedures and as specified in DDLs.

j. CPP military participants will wear their uniforms while CPP civilian participants will wear civilian attire in accordance with local command customs and tradition. They will wear, in clear view, a DA building or installation pass or badge (if required) that clearly identifies them as foreign nationals.

k. Any other identification (including organizational code and title, block, office nameplate, security badge, or email address) used by or issued to CPP participants by the host Army units will clearly identify the CPP participant's status as a foreign national. Email addresses will be in accordance with AR 25–2.

l. CPP participants will sign, as required, a statement regarding inventions rights.

N–3. Cooperative Program Personnel memorandum of agreement and certification

a. MOA. In lieu of AR 550–51, the streamlined procedures referenced in DODI 5000.02 and found in the Defense Acquisition Guidebook will be used for the development of international cooperative, research, development, and acquisition (ICRDA) agreements that authorize the establishment of CPP positions (see AR 70–41). The Cooperative Program and/or Project Annex or Article to an International Cooperative RDT&E and/or Acquisition Agreement or implementing arrangement thereto, will cover the following issues (at a minimum):

(1) Type of positions to be established.

(2) Length of tour.

(3) Financial responsibilities (for example, travel, salary, and so forth) and use of government facilities and equipment.

(4) Entitlements (for example, commissary privileges, medical care, and so forth).

(5) Status of assigned personnel, to include privileges and exemptions, liabilities and claims.

(6) Security.

(7) Disciplinary matters.

(8) Administrative matters and oversight responsibilities (for example, leave, dress, reviews, and performance reports).

(9) Identification.

b. Certification.

(1) CPP participants are certified to DA commands or agencies to perform assigned duties. Terms of certification are derived from and are consistent with the scope of the MOA.

(2) Each CPP participant must sign a certification statement acknowledging the terms of their assignment. A copy of the signed certification statement, which will be maintained by the local FDO, must be provided to the CPP with copies to the ACOM, ASCC, and/or DRU FDO, ASA (ALT) and DCS, G–2. If the CPP participant refuses to sign the certification statement, the command or agency must immediately notify the program manager who will resolve the issue through the parent government's military attaché in Washington, DC.

N–4. Establishment of Cooperative Program Personnel positions and processing of Cooperative Program Personnel nominations

a. Establishment of CPP positions. DA commands and agencies desiring to have CPPs certified and assigned to them must formally obtain HQDA concurrence. A request for a new CPP position will not be finalized unless the respective foreign government has signed an international MOA. A DDL is required for all CPP positions. The procedures for establishing a new CPP position are as follows:

(1) Request Initiated by a Foreign Government for Establishment of a CPP position.

(a) Step 1: If a foreign government initiates a request for the establishment of a CPP position with the Army, DASA (DE&C), HQDA will notify the affected command or agency in writing and request a recommendation on the establishment of the proposed CPP position. Such proposals will be conveyed in writing through command or agency channels. For example, if the request involves the assignment of a CPP to a PEO PM office, DASA (DE&C), HQDA will send the proposal to ASA (ALT) for staffing to the appropriate PEO PM.

(b) Step 2: The specified DA command or agency will evaluate the proposal and submit to DASA (DE&C), HQDA a recommendation to approve or disapprove the proposal. If the proposal involves the assignment of a CPP to the office of a PEO PM, the PM will coordinate their position with the ACOM, ASCC, or DRU matrix support and submit the coordinated position to ASA (ALT), which will forward the response to DASA (DE&C), HQDA. CPP position proposals must provide:

1. Position Description. A position description will be prepared for each CPP position. The position description will contain as a minimum:

a. Title of the position.

b. Position location.

c. Qualification and skills required.

d. Description of specific duties of the position.

e. Classified access level required.

f. Draft DDL.

2. Clearly demonstrate or anticipate a mutual need for the position. The rationale must clearly demonstrate the requirement for the CPP's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve the best interests of the Army.

(c) Step 3: DASA (DE&C), HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: DCS, G–2, ASA (ALT), DCS, G–3/5/7, Office of the Judge Advocate General (OTJAG), and the subject matter expert, if different from the preceding offices.

(d) Step 4: After HQDA coordination is completed, DASA (DE&C), HQDA will finalize the decision on the proposal and formally notify the appropriate foreign government embassy. If the proposal is approved, the DA command or agency to which the CPP will be assigned will immediately begin to finalize the position DDL for approval and issuance by DCS, G–2, HQDA. Upon concurrence and approval of the DDL, DASA (DE&C), HQDA, will notify the hosting Army command or agency and the appropriate foreign military attaché. The approved DDL will be in place prior to the submission of the EVA request by the appropriate foreign military attaché.

(2) Request Initiated by a DA Command or Agency for Establishment of a CPP position.

(a) Step 1: Prior to beginning discussions with foreign representatives on the establishment of a CPP position, DA commands or agencies must obtain DASA (DE&C), HQDA permission to proceed. Such proposals will be conveyed in

writing through command or agency channels to DASA (DE&C), HQDA. Proposals conveyed through PEO PMs will be sent to ASA (ALT) for forwarding to DASA (DE&C), HQDA.

(b) Step 2: A DA command or agency will provide the following information in support of its initiative to establish a CPP position:

1. Position Description. A position description will be prepared for each CPP position. The position description will contain as a minimum:

a. Title of the position.

b. Position location.

c. Qualification and skills required.

d. Description of specific duties of the position.

e. Classified access level required.

f. Draft DDL.

2. Clear statement of need for the position. The rationale must clearly demonstrate the requirement for the CPP's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished through a recurring visit request. The proposed position must clearly serve the best interests of the Army.

(c) Step 3: DASA (DE&C), HQDA will coordinate the proposal within HQDA and with the following offices at a minimum: DCS, G–2, ASA (ALT), DCS, G–3/5/7, OTJAG, and the subject matter expert, if different from the preceding offices.

(d) Step 4: After HQDA coordination is completed, DASA (DE&C) 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, DASA (DE&C) will direct the negotiations for DA. While the negotiations are being conducted, the DA command or agency that initiated the proposal will immediately begin to finalize the draft position DDL for approval and issuance by DCS, G–2, HQDA. Upon concurrence and approval of the DDL, DCS, G–2, HQDA will hold the document, awaiting conclusion of the negotiations and formal agreement to establish a CPP position. Upon establishment of the CPP position, the approved DDL will already be in place awaiting the submission of the EVA request by the appropriate foreign military attaché.

b. Processing of CPP nominations. If the CPP position is established, DCS, G–2, HQDA will process the assignment of the CPP 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 and/or assignment of the CPP. In the EVA request, the foreign military attaché provides written notification to DCS, G–2, HQDA of the following:

(a) Subject individual is an officially-sponsored official of that government.

(b) Such official is authorized by the sponsoring government to perform duties under a MOA.

(c) The official holds a specified level of security clearance.

(d) The parent government will assume the responsibility for any and all U.S. CMI provided to the CPP.

(2) Step 2: DCS, G–2, HQDA will process the EVA request to the program manager and the DA command or agency (PEO PM through its matrix support) to which the CPP is to be assigned. Since the DDL outlining the terms of the certification of the CPP was pre-coordinated and approved, the recipient DA command or agency should respond favorably within the required suspense assigned to the EVA request. See appendix D for detailed information on DDLs.

(3) Step 3: Upon receipt of the concurrence of the program manager and the recipient DA command or agency and receipt of the required photograph and biography from the foreign military attaché, DCS, G–2, HQDA will approve the EVA request and notify the program manager and the recipient DA command or agency of the approval. The foreign military attaché will then coordinate with the recipient DA command or agency for the arrival of the CPP.

c. DA commands or agencies may not accept a CPP until the DDL and visit request have been approved. If a CPP arrives prior to visit approval, the DA command or agency involved will not permit the CPP to commence their duties. The DA command or agency FDO must be notified immediately. The DA command or agency FDO will then notify the DCS, G–2, HQDA, who will coordinate the disposition of CPP with DASA (DE&C) and the appropriate foreign military attaché, and provide instructions to the DA command or agency FDO.

d. Modification of a CPP position. Any proposal to change the scope of a CPP's certification will be in accordance with the procedures outlined in paragraph N–4*a*, with emphasis on the specific modification. Any proposal to extend the CPP's duration must be initiated and requested by the appropriate foreign military attaché utilizing the FVS or by letter, if the embassy is not on FVS. Under "purpose of visit request" section of the extension request, appropriate foreign military attaché will state "extension of current visit" citing the existing visit request number.

e. Reevaluation of a CPP position. Once established, each CPP position and the associated DDL will be reevaluated on each successive nomination to ensure that the best interests of the host command or agency and DA continue to be served, and the purpose of the position remains valid. To alleviate the possibility of a CPP arriving to assume an established position prior to visit approval, DCS, G–2, HQDA will initiate contact with the appropriate foreign government Military Attaché in Washington, DC 90 days prior to the tour expiration date of the incumbent CPP and

query the foreign military attaché concerning a replacement for the position, extension of the incumbent CPP, or other alternatives contemplated by the parent government. The DCS, G–2, HQDA will also inform the sponsoring Army command or agency of the intended action, if any, of the foreign government to alter the status of the CPP position. The host command or agency FDO and contact officer will also commence their reevaluation 90 days prior to the tour expiration date of the incumbent CPP.

N–5. Administering Cooperative Program Personnel participants

a. Visits. All DA-directed visits or travel by the CPP participant will be in accordance with the standing operating procedures of the command or agency of assignment. However, all travel orders will identify the individual as a CPP participant assigned to the Army. DASA (DE&C) approval is required for all OCONUS travel by any CPP participant.

b. Library and publications support. At the discretion of the host activity, a CPP may be granted supervised access to the CMI section of a command or agency library. Additionally, each CPP may be provided a reference set of DA and activity publications necessary to the successful performance of the CPP's duties, consistent with the CPP's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the CPP's successor when the CPP's certification ends.

c. Computer access. CPPs may not have unsupervised access to computer systems (stand-alone or network) unless the information accessible by the computer is needed to accomplish the work under their approved position description and is authorized for disclosure to their government. In all cases, the provisions of AR 25–2 and local security procedures will apply.

d. Misconduct. CPP participants serve at the pleasure of DA and 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 CPP violates the terms of certification; violates applicable law, DOD, DA, or local regulatory guidance, or otherwise conducts personal or professional affairs in an unsatisfactory manner, the hosting command will provide a written report regarding the inappropriate action through proper channels (see para I–15). Those instances of personal misconduct will be reported to DASA (DE&C), in a timely manner, with the details of the corrective action taken or a recommendation for final disposition, such as temporary suspension or permanent revocation of privileges, or revocation of certification. DASA (DE&C) will provide DCS, G–2, HQDA with a copy of the report and coordinate the resolution of all misconduct cases.

N–6. Foreign disclosure officer

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

a. Assisting in the development of the DDL associated with each CPP position established within their respective command or agency.

b. Providing a position on the RVA request in accordance with the assigned suspense.

c. Providing advice and assistance on all matters pertaining to the disclosure of CMI to each CPP position assigned to the respective command or agency.

d. Maintaining a copy of the CPP certification statement.

e. Notifying the CPP Program Manager through command channels of any CPP misconduct.

f. Briefing CPP Contact Officer on their duties.

N–7. Supervisor functions

DA officials designated to supervise a CPP participant will—

a. Ensure that the CPP participant understands the duties to be performed in the assigned position.

b. Ensure that the CPP participant is provided access only to that CMI and CUI necessary to fulfill the duties of the position description as described in the DDL.

c. Be familiar with this regulation, other applicable regulatory guidance governing the disclosure of CUI, and specific disclosure guidelines established in the DDL.

d. Inform co-workers of the disclosure limitations on access to CMI and CUI related to the CPP participant and their responsibilities in dealing with the CPP participant.

e. Ensure that the CPP participant signs a certification before being assigned to the position.

f. Ensure the DDL is not provided to the ESEP participant. The DDL is a U.S. eyes-only document. See paragraph D–5 of this regulation.

N–8. United States contact officer

The responsibilities outlined in paragraphs O–2 and O–6 of this regulation apply.

Appendix O
Contact Officer and Visit Point of Contact Responsibilities

O–1. Concept

Contact officers will be designated in writing to facilitate and oversee activities of all extended foreign visitors (that is, FLOs, PEPs, ESEPs, CPPs, and so forth) at DA commands or agencies. Contact officers will be accessible to the extended foreign visitors. 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 their duties.

Note. For the purposes of this regulation, accessible is defined as being available, either in person, by telephone, or some other means to resolve issues, answer questions, give guidance, and so forth, as necessary for the conduct of the extended visitor's official activities.

O–2. General contact officer responsibilities

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 section, which may be supplemented, as necessary, to meet local requirements. Contact officers for extended foreign visitors 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 assignment.

c. Coordinate with and obtain guidance from the following agency or command personnel:

(1) FDO (concerning the preparation of briefings or discussion items in oral, visual, or documentary form).

(2) Security manager or operations security (OPSEC) officer (concerning agency or command activities from which extended visitors should be excluded). Escorts are required when the extended visitors cannot otherwise be denied access to information or operations outside the scope of the approved DDL.

(3) Protocol officer (concerning local policies regarding mandatory courtesy calls or exchange of mementos).

d. Prepare to receive and respond to confirmation of the extended visit request and a possible request for administrative assistance by the extended visitors or their military attachés.

e. On request, assist in arranging for quarters or transportation; however, it must be made clear to the extended visitors or their military attachés that all expenses concerning the visit, including quarters, transportation, and subsistence, are the responsibility of the extended visitors. Contact officers should refrain from making commercial reservations for services on behalf of extended foreign visitors; rather, assistance should be limited to recommending and providing telephone numbers for commercial services to foreign visitors or their military attachés.

f. Ensure that extended foreign visitors are aware of and comply with foreign disclosure and security requirements regarding the assignment.

g. Make personnel with whom extended visitors have official contact or exchange information fully aware of information disclosure guidance and restrictions applicable to the assignment.

h. Notify the supporting counterintelligence office of any extended foreign visitor activity that is reportable under the provisions of AR 381–12.

i. In the event of any misconduct on the part of an extended foreign visitor during their assignment that is outside of the activities reportable under AR 381–12 (see para I–15), provide a written report to DCS, G–2 through command channels.

j. Complete an Army Contact Officer Certification Course and provide proof of completion to the servicing FDO.

O–3. Contact officer responsibilities for foreign liaison officers

a. Contact officers who oversee the activities of FLOs should be of equivalent rank or 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 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 their duties. Contact officers will also comply with the guidelines listed below.

b. In addition to those responsibilities outlined in paragraph O–2, 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 for the individual FLO position.

(2) Initially brief a new FLO on DA and local policies and procedures affecting their status and performance of functions, as well as customs of the 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 their 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 and/or refer all FLO requests for CMI to the FDO.

(5) Notify the DCS, 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 (see para I–15).

(7) Comply with the procedures cited in paragraph J–6 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.

O–4. Contact officer responsibilities for Military Personnel Exchange Programs

a. Contact officers who oversee the activities of MPEPs at DA commands or agencies should be of equivalent rank or grade or higher, if available, to the MPEP. A primary and an alternate contact officer must be identified in the DDL. They must be accessible to and have daily contact with the MPEP. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of their duties. Contact officers will also adhere to the guidelines listed below.

Note. In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the Army.

b. In addition to those responsibilities outlined in paragraph O–2, the contact officer for a MPEP will—

(1) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by DCS, G–2, HQDA for the individual MPEP position.

(2) Initially brief a new MPEP on DA and local policies and procedures affecting the MPEP's status and performance of functions, as well as customs of the Army; subsequently, the contact officer will render advice and assistance to the MPEP in complying with such policies and procedures. The contact officer will have the MPEP sign a certification statement indicating their agreement and understanding. The contact officer will provide a copy of the signed certification form to the MPEP.

(3) In conjunction with the FDO, evaluate the MPEP's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the MPEP's approved terms of certification. Consultations and visits beyond a MPEP's terms of certification require the submission of formal visit requests by the MPEP's embassy in Washington, DC.

(4) Receive, evaluate, and recommend and/or refer all MPEP requests for CMI to the FDO.

(5) Receive, evaluate, and refer all MPEP requests involving CUI in accordance with ACOM, ASCC, or DRU procedures.

(6) Notify the DCS, G–2, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of MPEPs under their oversight.

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

(8) Comply with the procedures cited in paragraph L–5*d* of this regulation regarding misconduct on the part of the MPEP.

(9) Brief U.S. personnel with whom the MPEP will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

O–5. Contact officer responsibilities for Engineers and Scientists Exchange Programs

a. Contact officers who oversee the activities of ESEPs at DA commands or agencies should be of equivalent rank or grade or higher, if available, to the ESEP. A primary and an alternate contact officer must be identified in the DDL. They must be accessible to and have daily contact with the ESEP. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of their duties. Contact officers will also adhere to the guidelines listed below.

Note. In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the Army.

b. In addition to those responsibilities outlined in paragraph O–2, the contact officer for a ESEP will—

(1) Be briefed by the FDO and become familiar with this regulation and the specific terms of certification approved by DCS, G–2, HQDA for the individual ESEP position.

(2) Initially brief a new ESEP on DA and local policies and procedures affecting the ESEP's status and performance

of functions, as well as customs of the Army; subsequently, the contact officer will render advice and assistance to the ESEP in complying with such policies and procedures. The contact officer will have the ESEP sign a statement indicating their agreement and understanding. The contact officer will provide a copy of the signed certification form to the ESEP participant and the Army lead agent.

(3) In conjunction with the FDO, evaluate the ESEP's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the ESEP's approved terms of certification. Consultations and visits beyond a ESEP's terms of certification require the submission of formal visit requests by the ESEP's embassy in Washington, DC.

(4) Receive, evaluate, and recommend and/or refer all ESEP requests for CMI to the FDO.

(5) Receive, evaluate, and refer all ESEP requests involving CUI in accordance with local procedures.

(6) Notify the DCS, G–2, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of ESEPs under their oversight.

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

(8) Comply with the procedures cited in paragraph M–5*d* of this regulation regarding misconduct on the part of the ESEP.

(9) Brief U.S. personnel with whom the ESEP will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

O–6. Contact officer responsibilities for Cooperative Program Personnel

a. Contact officers who oversee the activities of CPPs at DA commands or agencies should be of equivalent rank or grade or higher, if available, to the CPP. A primary and an alternate contact officer must be identified in the DDL. They must be accessible to and have daily contact with the CPP. All contact officers must be familiar with this regulation, other applicable guidelines governing the disclosure of CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of their duties. Contact officers will also adhere to the guidelines listed below.

Note. In all cases, Army commands or agencies will not assign the duties of a contact officer to U.S. contractors, unless it is specifically written in their contract that they are official representatives of the Army.

b. In addition to those responsibilities outlined in paragraph O–2, the contact officer for a CPP will—

(1) Be briefed by the FDO and become familiar with this regulation and the specific terms of certification approved by DCS, G–2, HQDA for the individual CPP position.

(2) Initially brief a new CPP on DA and local policies and procedures affecting the CPP's status and performance of functions, as well as customs of the Army; subsequently, the contact officer will render advice and assistance to the CPP in complying with such policies and procedures. The contact officer will have the CPP sign a statement indicating their agreement and understanding. The contact officer will provide a copy of the signed certification form to the CPP.

(3) In conjunction with the FDO, evaluate the CPP's requests for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent with the CPP's approved terms of certification. Consultations and visits beyond a CPP's terms of certification require the submission of formal visit requests by the CPP's embassy in Washington, DC.

(4) Receive, evaluate, and recommend and/or refer all CPP requests for CMI to the FDO.

(5) Receive, evaluate, and refer all CPP requests involving CUI in accordance with local procedures.

(6) Notify the DCS, G–2, HQDA through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of CPPs under their oversight.

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

(8) Comply with the procedures cited in paragraph N–5*d* of this regulation regarding misconduct on the part of the CPP.

(9) Brief U.S. personnel with whom the CPP will have official contact, to include one-time and recurring visits external to the command or agency, to ensure that they are made fully aware of disclosure guidance and restrictions.

O–7. Visit point of contact responsibilities

Visit POCs are assigned for one-time and recurring visiting foreign representatives and will adhere to the guidelines listed below. As a minimum, each visit POC is to perform the duties and functions outlined in this section, which may be supplemented, as necessary, to meet local requirements. Visit POCs for one-time and recurring visiting foreign representatives will—

a. Become familiar with chapters 1 through 3 and appendix I 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 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, visit POCs 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 that is outside of the activities reportable under AR 381–12 (see para I–15), provide a written report to DCS, G–2 through command channels.

Appendix P
Internal Control Evaluation and Department of the Army Staff Assistance and Compliance Visits

P–1. Function

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

P–2. Purpose

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

P–3. Instructions

The checklist below must be based on the actual testing of key internal 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 internal controls must be officially evaluated at least once every five years. Commands and agencies will certify that a required internal control evaluation has been conducted and will be documented on DA Form 11–2 (Internal Control Evaluation Certification) in accordance with AR 11–2.

P–4. Test questions

a. Has the FDO been appointed in writing (see para 2–11*a*(1))? Has a copy been provided to the ACOM, ASCC, or DRU (see para 2–11*a*(1))?

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

(1) AR 380–5.

(2) DODD 5230.11.

(3) DODD 5230.20.

c. Has the FDO completed an Army Foreign Disclosure Certification Course (see para 2–11*a*(2))?

d. Have foreign representatives been properly certified to the command or agency (see apps J through N)?

e. Have activities that foreign government officials have conducted, that are outside of the terms of certification, been reported to the FDO and HQDA (see paras J–5*b*, K–4, L–5*d*, M–5*d*, and N–5*d*)?

f. Does the contact officer maintain DDLs on all foreign representatives assigned to them (see para D–4)?

g. Have contact officers been designated in writing to control the activities of foreign visitors (see paras 2–11*c* and O–1)?

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 app O)?

i. Are DDLs prepared for each assigned foreign representative (see para D–3*a*)?

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 2–13)?

m. Are SPAN entries being made for CMI disclosures within 20 days of the actual first-time disclosure (see para 3–8*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 2–8*b*)?

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 visit 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 or non-sponsored (see paras I–12*c*(3)(c)5 and I–12*d*(2))?

s. Did contact officers receive guidance from the FDO regarding visits that will involve the disclosure of U.S. CMI (see para O–1 and O–2)?

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 O–2 through O–6)?

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

P–5. Supersession

This checklist replaces the checklist previously published in AR 380–10, dated 22 June 2005.

P–6. Comments

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

Glossary

Section I
Abbreviations

ABCA
American, British, Canadian, Australian, and New Zealand Armies

ACOM
Army command

AECA
Arms Export Control Act

AMC
Army Materiel Command

APD
Army Publishing Directorate

APEP
Administrative and Professional Personnel Exchange Program

AR
Army regulation

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

ASCC
Army service component command

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

CLO
Country Liaison Officer

CMI
classified military information

CNGB
Chief, National Guard Bureau

COE
Chief of Engineers

COMSEC
communications security

CONUS
continental United States

CPI
critical program information

CPP
cooperative program personnel

CSA
Chief of Staff, Army

CUI
controlled unclassified information

DA
Department of the Army

DASA (DE&C)
Deputy Assistant Secretary of the Army for Defense Exports and Cooperation

DCS
direct commercial sales

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3/5/7
Deputy Chief of Staff, G–3/5/7

DCS, G–4
Deputy Chief of Staff, G–4

DCS, G–8
Deputy Chief of Staff, G–8

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

DOTMLPF
doctrine, organization, training, materiel, leadership and education, personnel, and facilities

DRU
direct reporting unit

DSS
Defense Security Service

DTIC
Defense Technical Information Center

EAR
Export Administration Regulations

ECP
engineering change proposal

ENDP
exception to the National Disclosure Policy

EO
executive order

ESEP
Engineer and Scientist Exchange Program

EVA
extended visit authorization

FDO
foreign disclosure officer

FDR
foreign disclosure representative

FDS
Foreign Disclosure System

FLO
foreign liaison officer

FMS
foreign military sales

FOIA
Freedom of Information Act

FVS
Foreign Visits System

GPO
Government Printing Office

GSOMIA
General Security of Military Information Agreement

HQDA
Headquarters, Department of the Army

ICRDA
International cooperative research, development, and acquisition

IEA
information exchange annex

IMET
International Military Education and Training

INSCOM
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

MCTL
Militarily Critical Technology List

MFC
multinational force compatibility

MOA
memorandum of agreement

MOU
memorandum of understanding

MPEP
military personnel exchange program

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

NGB
National Guard Bureau

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

OCA
original classification authority

OCONUS
outside the continental United States

OPSEC
operations security

OSD
Office of the Secretary of Defense

OTJAG
Office of the Judge Advocate General

P&A
price and availability

Pam
pamphlet

PEO
program executive office

PEP
personnel exchange program

PIP
product improvement proposal

PM
program manager

POC
point of contact

PPP
program protection plan

RA
record of action

R&D
research and development

RDT&E
research, development, test, and evaluation

RFI
request for information

RFP
request for proposal

RVA
request for visit authorization

SCI
sensitive compartmented information

SIPRNET
Secure Internet Protocol Router Network

SPAN
Security Policy Automation Network

SSOI
summary statement of intent

StanList
standardization list

StanRep
standardization representative

TA/CP
technology assessment/control plan

TJAG
The Judge Advocate General

TPO
technical project officer

TRADOC
Training and Doctrine Command

TRDP
technology research and development program

TSG
The Surgeon General

TTCP
The Technology Cooperation Program

U.S.
United States

USACIDC
U.S. Army Criminal Investigation Command

USASAC
U.S. Army Security Assistance Command

USC
United States Code

USDAO
United States Defense Attaché Office

USG
United States Government

VCSA
Vice Chief of Staff, Army

Section II
Terms

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.

Army exchange personnel
Military or civilian officials of the 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.

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 fundamental applied research to sophisticated breadboard hardware, study, programming and planning efforts that establish the initial feasibility and practicality of proposed solutions to technological challenges. It would thus include studies, investigations, and non-system-specific development efforts. 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 13526 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 member designated in writing to oversee and facilitate all contacts, requests for information, consultations, access, and other activities of foreign nationals who are assigned to 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
A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification in accordance with Executive Order 13526, but is pertinent to the national interests of the U.S. or to the important interests of entities outside the Federal Government and under law or policy requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

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.

Country Liaison Officer
An officer or non-commissioned officer of a foreign military establishment selected by their government and attached to a DOD or civilian activity for the primary purpose of assisting in the administration of international military students from the home country.

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 and/or 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 and/or 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 their organization to foreign governments and international organizations.

Disclosure
Conveying information, in any form or manner, to an authorized representative of a foreign government, foreign entity supporting U.S. interests and/or security objectives or international organization. Disclosures may be accomplished through oral, visual, or documentary modes.

a. Oral disclosure refers to the ability to convey information through conversation. The limiting factor is that information that can be conveyed through speech.

b. Visual disclosure refers to the ability to actually show the information. Visual disclosure also allows study and analysis of the information.

c. Documentary disclosure (also referred to as Release by the intelligence community) refers to the ability and authority to convey permanent physical custody and/or transfer of the information to be disclosed.

Disclosure Program
A program under which information and materiel are evaluated for the disclosure or potential disclosure of classified military information. Such programs must be evaluated in their entirety, from beginning to end and include all potential disclosures of classified military information in all NDP–1 disclosure categories.

Document and/or documentary materiel
Any recorded information, regardless of its medium, physical form, or characteristics.

Documentary disclosure
See disclosure.

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.

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-originated, developed, or derived CMI.

Foreign disclosure representative
An individual designated in writing to assist and advise the command FDO on all disclosure matters. FDRs can be either DA members or contractor personnel. FDRs may be appointed at any level of command. FDRs may not make disclosure decisions

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

Foreign government 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 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 U.S. or its possessions and trust territories; and any person who is not a citizen or national of the U.S.

Foreign liaison officer
A foreign government military member or civilian employee who is authorized by their government to act as an official representative of that government in its dealings with the Army in connection with programs, projects, or agreements of mutual interest to the 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 their 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 U.S. or its territories. This definition does not include permanent residents (formerly immigrant aliens, resident aliens, or intending U.S. citizens). For the purposes of this regulation, a private non-U.S. citizen or national having no official affiliation with their government of origin. See definition of foreign government representative.

Foreign representative
See foreign government representative.

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.

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).

Information
Knowledge in a communicable form.

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.

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 MFC among NATO and ABCA member nations and MOUs providing for cooperative R&D, including codevelopment, dual production, defense data exchange programs, 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.

a. 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.

b. 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.

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.

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

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 Army. The document may include authorization for a foreign military attaché to affect direct contact with DA officials of a specified DA command or agency without prior permission of HQDA (DCS, 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.)

Multinational force compatibility
The collection of capabilities, relationships, and processes that together enable the Army to conduct effective coalition operations across the full spectrum of military missions. It encompasses not only the capability to conduct effective military operations with coalition partners, but also the factors that contribute to the development and maintenance of a coalition relationship. It is directly affected by and implemented through activities and changes throughout the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) spectrum.

Munitions license
A document bearing the word license, issued by the Director, Office of Defense Trade Controls or their 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, disclosure 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.

Oral disclosure
See disclosure.

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

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.

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 affected without the owner's consent unless such disclosure is authorized by relevant legislation, and then disclosure will be subject to such legislation.

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 their government for access to information of the security classification involved and that the recipient government will comply with security requirements specified by the U.S.

Security Policy Automation Network
A wide-area computer network sponsored by the Office of the Under Secretary of Defense (Policy) 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.

SENTRY
The Army's foreign disclosure support system which provides a secure, Web-based application that promotes a common operational picture for the Army foreign disclosure community and compliments and enforces existing DCS,

G–2 Foreign Disclosure Branch, business processes. The primary purpose for SENTRY is to serve as DA's official repository for all DA DDLs and certified visitors. Secondary uses of SENTRY include: providing the FDO Community with relevant information needed to address basic disclosure criteria when rendering disclosure decisions; and serving as a library for various resources (for example, security classification guides; directives, regulation, and guidance; program security documentation; National Disclosure Policy Records of Action; information on misconduct by visiting foreign representatives; and so forth) useful in the development of disclosure guidance.

Sponsorship
In the context of a meeting, provision of DA resources (such as personnel and funds) in support of the meeting.

a. 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).

b. 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 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 and/or data
Information, including scientific information, 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 U.S. As a condition of the original sale or transfer, the recipient government must obtain the consent of the President of the U.S. for any proposed third country and/or party transfer.

Training
Formal or informal instruction of foreign representatives in the U.S. or overseas either by officers or employees of the U.S., 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. 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)(3). 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 U.S. It also includes any governmental (Federal, State, or local) entity. It does not include any foreign person.

a. 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 U.S. as an immigrant according to the immigration laws, such status not having changed.

b. According to 8 USC 1324b(a)(30), the term protected individual means an individual who is a citizen or national of the U.S. 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 six months of the date the alien first becomes eligible (by virtue of period of lawful permanent residence) to apply for naturalization or, if later, within six months after November 6, 1986. The term also does not include an alien who has applied on a timely basis but has not been naturalized as a citizen within two 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 two-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 disclosed has been defined and approved for disclosure 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).

Visual disclosure
See disclosure.

Section III
Special Abbreviations and Terms

ODASA (DE&C)
Office of the Deputy Assistance Secretary of the Army for Defense Exports and Cooperation

USNORTHCOM
U.S. Northern Command