AR 380-10 cy.3

Army Regulation 380–10

Security

Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives

Headquarters
Department of the Army
Washington, DC
30 December 1994

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-10
Technology Transfer, Disclosure of Information and
Contacts with Foreign Representatives

This revision--

- Consolidates AR 380-10 and AR 380-66.
- Changes guidance to be consistent with Department of Defense Directive 5230.11 and Department of Defense Directive 5230.20.
- Changes the definition of Category 4 - Production Information to be consistent with changes in the National Disclosure Policy (table 4).
- Identifies and discusses the Technology Assessment/Control Plan and Program Protection Plan to be consistent with Department of Defense Directive Series 5000 (chap 2 and app C).
- Details procedures used by foreign embassies to request documents from the Army (chap 4).
- Clarifies Army policy concerning foreign liaison officers to Army commands and agencies (chap 5).
- Clarifies standards of appearance expected of foreign visitors to Department of the Army activities (chap 5).
- Incorporates procedures established by the U.S.-Canada Joint Certification Program for unclassified visits to DA elements and DA contractors by Canadian government officials and certified Canadian contractors (chap 5).

Headquarters
Department of the Army
Washington, DC
30 December 1994

*Army Regulation 380–10

Effective 31 January 1995

Security

Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

MILTON H. HAMILTON
Administrative Assistant to the Secretary of the Army

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

Summary. This regulation is a consolidation of AR 380-10 and AR 380-66. It provides policy regarding procedures for disclosure of Army classified military information and controlled unclassified information; policy regarding contacts with foreign representatives, encompassing visits by foreign nationals, certification of foreign liaison officers and foreign exchange personnel to Department of the Army commands, installations, and contractors, and industrial or military facilities for which the Department of the Army is the executive agent or has security cognizance; guidelines for foreign national attendance at Army-sponsored classified and unclassified meetings, conferences, and symposia; and establishes policy, prescribes procedures, and assigns responsibilities for controlling the direct and indirect international transfer of critical military technology. This regulation implements DOD Directive 2040.2, DOD Directive 5230.11, and DOD Directive 5230.20.

Applicability. This regulation applies to the Active Army, the Army National Guard, and the U.S. Army Reserve. It applies to all personnel involved in the foreign disclosure and technology transfer process, to include but not limited to the disclosure of classified military information and controlled unclassified information, visits, conferences, symposiums, and meetings involving foreign personnel, as well as certification of liaison officers and exchange personnel. This regulation is applicable up to and during full mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence (DCSINT). The DCSINT has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this authority, in writing, to a division chief under their supervision, within the proponent agency who holds the grade of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions in accordance with AR 11-2, but does not contain checklists for assessing management controls. Alternative management control reviews are used to accomplish assessment of managment controls.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (DAMI-CIT), WASH DC 20310-1057.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIT) WASH DC 20310-1057.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12-09-E, block number 1023, intended for command levels C, D, and E for the Active Army, the Army National Guard, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1
General, *page 1*

Section I
Introduction, page 1
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Objectives • 1–4, *page 1*
Policy • 1–5, *page 1*

Section II
Responsibilities, page 2
HQDA Deputy Chief of Staff for Intelligence (DCSINT) • 1–6, *page 2*
Heads of HQDA Staff Agencies and MACOM Commanders • 1–7, *page 3*
HQDA Deputy Chief of Staff for Logistics (DCSLOG) • 1–8, *page 3*
HQDA Deputy Chief of Staff for Operations and Plans (DCSOPS) • 1–9, *page 3*
Assistant Secretary of the Army (Research, Development and Acquisition)(ASA(RDA)) • 1–10, *page 3*
Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM) • 1–11, *page 4*
Commanding General, U.S. Army Materiel Command (CG, AMC) • 1–12, *page 4*
The Judge Advocate General (TJAG) • 1–13, *page 4*
The Surgeon General (TSG), the Chief of Engineers (COE), and the Director, Information Systems for Command, Control, Communications and Computers (DISC4) • 1–14, *page 4*
Directors and Commanders of Army Laboratories, R&D Centers, and Other R&D Activities • 1–15, *page 4*

*This regulation supersedes AR 380-10, 29 July 1988 and AR 380-66, 23 October 1987, and rescinds DD Form 1823.

UNCLASSIFIED

CG, U.S. Army Criminal Investigation Command (USACIDC) • 1–16, *page 4*
Overseas major commanders • 1–17, *page 4*
Other Overseas Army Activities • 1–18, *page 5*

Section III
Categorization, Disclosure and Funding Procedures, page 5
Categorization of Military Information by Sensitivity • 1–19, *page 5*
Categorization of military information by nature and type • 1–20, *page 5*
Designated disclosure channels • 1–21, *page 5*
Security protection and assurances • 1–22, *page 6*
Security Classification Guidance for DA Foreign Disclosure Activities • 1–23, *page 6*
Nature of contacts with foreign representatives • 1–24, *page 6*
Channels of official communication • 1–25, *page 6*
Funding and other support rendered to foreign representatives • 1–26, *page 6*

Chapter 2
General Disclosure Policies, Authority to Disclose, and Delegation of Authority Introduction, *page 7*

Section I
Introduction, page 7
Concept • 2–1, *page 7*
False impressions • 2–2, *page 7*
Maximum classification disclosure levels • 2–3, *page 8*
Basic disclosure criteria • 2–4, *page 8*
Disclosure conditions • 2–5, *page 8*
Disclosure limitations • 2–6, *page 9*
Establishment of Disclosure Programs • 2–7, *page 9*
International technology transfer policy • 2–8, *page 9*
DA contractor functions • 2–9, *page 10*

Section II
Authority to Disclose Classified Military Information (CMI) and Controlled Unclassified Information (CUI) and Delegation of Disclosure Authority, page 10
CUI Disclosure Authority and Delegation of Authority • 2–10, *page 10*
CMI disclosure authority and delegation of authority • 2–11, *page 11*
Authority to release CMI and CUI • 2–12, *page 12*
Authority to deny foreign disclosure of CMI and CUI • 2–13, *page 12*

Chapter 3
Policies and Procedures for Specific International Activities, *page 12*

Section I
Introduction, page 12
International activities (excluding security assistance actions) prompting CMI and CUI disclosures • 3–1, *page 12*
Coordination of proposed disclosures • 3–2, *page 12*

Section II
Security Assistance-related Disclosure of CMI and CUI, page 13
Concept • 3–3, *page 13*
Disclosure of CMI and CUI on a security assistance basis • 3–4, *page 13*
Disclosure of CMI and CUI on a licensed commercial basis • 3–5, *page 14*
Foreign test and evaluation of materiel • 3–6, *page 14*
Disclosure of CMI and CUI in Security Assistance-Related Training • 3–7, *page 15*

Section III
Research and Development (R&D) Materiel-Related Disclosure of CMI and CUI, page 15
Concept • 3–8, *page 15*
Preparation and implementation of International Cooperative R&D Agreements • 3–9, *page 15*
CMI and CUI disclosure regarding materiel changes and improvements • 3–10, *page 16*
CMI and CUI disclosure to foreign personnel integrated into the DA R&D structure • 3–11, *page 16*
Foreign participation in classified contracts • 3–12, *page 16*

Chapter 4
Modes, Methods, and Channels for CMI and CUI Release and Related Administrative Procedures, *page 16*

Section I
Procedures for Release to or by Visitor, Exchange, and Liaison Personnel, page 16
Introduction • 4–1, *page 16*
DA CMI and CUI released during visits • 4–2, *page 17*
DA CMI and CUI released to or by exchange personnel • 4–3, *page 17*
A CMI and CUI released to or by certified liaison officers • 4–4, *page 17*
DTIC document requests from specified governments • 4–5, *page 18*
JCO-certified contractors • 4–6, *page 18*
Other Releases of DA CMI and CUI • 4–7, *page 18*

Section II
Administration, page 19
Concept • 4–8, *page 19*
Physically conveying documentary material • 4–9, *page 19*
Recording CMI and CUI disclosure determinations and releases • 4–10, *page 20*

Chapter 5
Contact with Foreign Representatives, *page 21*

Section I
General Policy, page 21
Encounters with foreign representatives • 5–1, *page 21*
Military attaches • 5–2, *page 21*
Disclosure of information • 5–3, *page 21*
Delegation of Disclosure Letter • 5–4, *page 21*
Standards of appearance • 5–5, *page 21*
Contact officer • 5–6, *page 21*
Access to DA facilities • 5–7, *page 22*

Section II
DA International Visits Program, page 22
Concept • 5–8, *page 22*
Foreign Visits System (FVS) requirements • 5–9, *page 22*
Requests from countries without a military attache • 5–10, *page 23*
Foreign-owned U.S. companies • 5–11, *page 23*
Out of channel visit requests • 5–12, *page 23*
U.S.-sponsored visits • 5–13, *page 23*
Invitations and other prior coordination • 5–14, *page 24*
Functions in honor of or sponsored by foreign nationals • 5–15, *page 24*
Requests for visit authorizations (RVAs) • 5–16, *page 25*
Assignment, evaluation, and processing of RVAs • 5–17, *page 25*
Visits by Foreign National Employees of U.S. Defense Contractors • 5–18, *page 27*
Visits for Foreign Participation in U.S. Procurement-Related Meetings • 5–19, *page 27*

Visits by Representatives of the North Atlantic Treaty Organization (NATO) • 5–20, *page 27*
Visits by Representatives of the American, British, Canadian, and Australian (ABCA) Program • 5–21, *page 27*
Canadian Visits Under the U.S.-Canada Joint Certification Program (JCP) • 5–22, *page 27*
Processing RVAs to attend meetings, conferences, and symposim • 5–23, *page 27*
Delegation of authority to approve certain visits by foreign representatives • 5–24, *page 27*

Section III
Liaison Officers, page 28
Concept • 5–25, *page 28*
Establishment of LNO positions • 5–26, *page 28*
Processing requests for liaison officer certification • 5–27, *page 29*
Administering liaison officers • 5–28, *page 29*

Section IV
Exchange Personnel, page 30
Concept • 5–29, *page 30*
Restrictions on exchange personnel • 5–30, *page 30*
Access limitations • 5–31, *page 31*
Delegation of Disclosure Letter • 5–32, *page 31*
Processing nominations of foreign personnel for exchange • 5–33, *page 31*
Administering exchange officers • 5–34, *page 31*
Temporary duty travel of foreign exchange personnel • 5–35, *page 32*
Supervisor functions • 5–36, *page 32*

Chapter 6
Meetings, Conferences and Symposia, *page 32*

Section I
Introduction, page 32
Approval policies • 6–1, *page 32*
Types of meetings • 6–2, *page 32*

Section II
Non-Acquisition-Related Meetings, page 32
Established Cooperative Programs • 6–3, *page 32*
Unclassified meetings • 6–4, *page 32*
Classified meetings • 6–5, *page 32*

Section III
Acquisition-Related Meetings, page 33
Rationalization, standardization, and interoperability • 6–6, *page 33*
Planning • 6–7, *page 33*
Procedures • 6–8, *page 33*

Appendixes

A. References, *page 36*
B. Exceptions to Policy, *page 37*
C. Technology Assessment/Control Plan (TA/CP), *page 39*
D. Delegation of Disclosure Authority Letter (DDL), *page 41*
E. Conditions of Release Statements, *page 45*
F. Sample Certification of Conditions and Responsibilities, *page 45*

Table List

Table 1–1: Security Classification Guide for Disclosure-Related Activities, *page 7*
Table 4–1: Document Request Procedures, *page 20*

Figure List

Figure 2–1. Political and Military Criteria, *page 12*
Figure 6–1. Guidelines for foreign participation in classified meetings, *page 35*
Figure B–1. Format for a Request for Exception to the NDP, *page 38*
Figure D–1. DDL for weapons system or data exchange annexes, *page 41*
Figure D–2. DDL for liaison officer and exchange officer, *page 43*
Figure F–1. Sample certification to be signed by foreign liaison officers, *page 45*
Figure F–2. Sample certification to be signed by exchange officers, *page 46*

Glossary

Index

RESERVED

Chapter 1
General

Section I
Introduction

1–1. Purpose

This regulation assigns responsibilities for the Army Technology Security Program, including identifying and assessing critical military technologies and for assessing factors that contribute to international technology control decisions. It delegates authority for routine international technology transfer decisions and defines channels for resolving unconventional technology transfer decisions.

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 special terms used in this regulation are explained in the glossary.

1–4. Objectives

a. Militarily critical technologies and items of intrinsic military utility are valuable limited national security resources that resulted from considerable expenditures of money, time, and effort. They must be protected to ensure the Army maintains a qualitative lead over potential opponents' warfighting capabilities. Consistent with this statement is the recognition of the importance of international trade and interoperability with our allies. The objectives of the Army technology security program are to—

(1) Manage international transfers of technologies, goods, services, and munitions consistent with U.S. foreign policy and national security objectives.

(2) Ensure international activities are carefully targeted and closely managed to enhance their efficiency and effectiveness and to extract maximum benefits for both the U.S. Army and the foreign participants without compromise of critical technologies.

(3) Focus counterintelligence support on the protection of critical technologies, critical information, and national defense information.

b. The exchange of information between the Department of the Army (DA) and the military establishment of allied and friendly foreign governments and international organizations is a necessary adjunct to successful participation of DA in international and functional agreements. Such exchange is also needed to satisfy U.S. mutual defense commitments. At the same time, the protection of classified and otherwise sensitive unclassified military information against disclosure to unauthorized persons whether U.S. or foreign is an equally necessary adjunct to the military security of the United States. Thus, the objectives of the Army foreign disclosure program are as follows:

(1) To interpret national and Department of Defense (DOD) foreign disclosure policies in a manner that readily correlates with DA international activities and to standardize DA procedures to promote both prompt and consistent implementation of those policies.

(2) To approve information for foreign disclosure only after such information has been fully evaluated against standardized criteria and it has been determined that such disclosure demonstrably would result in a net benefit to, or otherwise be in the best interest of the U.S. Government.

(3) To ensure information is released only to authorized and certified foreign representatives and in specific channels designated for that purpose, in order to satisfy legal and recordkeeping requirements.

c. The objective of the Army's policy on visits and certification is to balance the need for—

(1) Efficient interaction between foreign representatives and DA to achieve DA objectives in its various international activities, including NATO standardization and cooperative research and development (R&D) activities and projects; American, British, Canadian, and Australian (ABCA) standardization activities and projects; cooperative R&D agreements; security assistance; Senior National Representatives activities; and reciprocal defense procurement and offset purchase arrangements.

(2) Control of such interaction to ensure that the security interests of the Army are promoted and preserved.

1–5. Policy

a. This regulation prescribes DA policies and procedures governing the disclosure of information and contacts with foreign representatives, as outlined below.

(1) *Disclosure of information.* This regulation governs the disclosure of certain types of official DA information, identified herein, to representatives of foreign governments and international organizations (hereafter referred to as "foreign disclosure"). The kinds of information covered are listed below.

(a) Classified information. Information originated by or for DOD or its departments or agencies or under their jurisdiction or control, and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL, as described in Executive Order 12356 (hereafter "classified military information (CMI),") except for that information identified otherwise below. CMI may be in documentary, oral, visual, or materiel form. (See AR 380–5.)

(b) Controlled unclassified information. Unclassified information and technical data for which dissemination outside DA is controlled under AR 25–55, AR 70–11, AR 70–31, and AR 530–1, as well as that unclassified information which may not be exported lawfully without either an approved munitions license from the Department of State (see International Traffic in Arms Regulations (ITAR)) or a validated license from the Department of Commerce (see Export Administration Regulations (EAR)) (hereafter, "controlled unclassified information" or CUI). CUI is not releasable to the public at large, but may be requested through government-to-government channels.

(2) *Contacts with foreign representatives.* This regulation governs activities and actions involving representatives of foreign governments and international organizations as well as foreign personnel, who by the nature of their association with the U.S. Army, are not designated to officially represent their government for the purposes of exchanging CMI or CUI as listed below.

(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.

(b) Liaison officers. Foreign government officials, either military or civilian employees, who are designated by their governments to act as a representatives of that government to an Army component in connection with bilateral or multilateral programs or projects.

(c) Exchange personnel. Foreign military personnel under the Personnel Exchange Program (PEP) or civilian and military personnel under the Scientist and Engineer Exchange Program (SEEP) who, with the exception of specific security requirements, are integrated into the U.S. Army.

(d) Meetings, conferences, and symposia. Attendance by foreign nationals or their representatives at meetings, conferences, and symposia sponsored or hosted by DA. (See AR 380–5.)

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

(1) Determine releasability 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 duties and responsibilities of personnel designated as Army contact officers, for foreign representatives who are visiting, certified as liaison officers, or assigned as exchange personnel to DA elements.

d. This regulation does not govern the foreign disclosure of certain types of information including intelligence information, the dissemination of which is handled through other than Army channels. These types of information are listed below.

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

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

(3) *Counterintelligence.* Counterintelligence operational information.

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

(5) *Strategic information.* Strategic planning information and related guidance, as designated by the Joint Chiefs of Staff (JCS). (See Chairman of the Joint Chiefs of Staff Memorandum of Policy (CJCS MOP) Number 60.)

(6) *Communications security.* Equipment or information relating to communications security (COMSEC), such as cryptographic devices and systems. (See AR 380–40 and DA Pam 25–380–2.)

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

(8) *Automated Information Systems information in OCONUS environment.* Unclassified information which has been, is, or can be deemed suitable for disclosure to local nationals employed in overseas U.S. Army computer/communications facilities according to AR 380–19.

(9) *Special access programs.* Information covered under special access programs.

(10) *Information to Anyone Who does not Qualify as a "Foreign Representative."* Any information released to U.S. citizens and immigrant aliens or intending citizens (formerly "resident aliens"), except such persons who have been identified as "foreign representatives" (see glossary). For U.S. citizens, immigrant aliens, and intending citizens, access to CMI is governed by AR 380–5 and access to CUI by AR 25–55, AR 70–11, AR 70–31, and AR 70–57.

(11) *Privacy Act information.* Information withheld from public disclosure under the Privacy Act, according to AR 340–21.

(12) *Information in the Public Domain.* Unclassified information that has been, is, or can be deemed suitable for disclosure to the public at large, in accordance with AR 70–11 and AR 360–5. Foreign governments can purchase public domain information from the Government Printing Office, Washington, DC and from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22151.

(13) *Export of Information Governed by the Department of Commerce.* Scientific, educational, or other data that qualify for general license under Department of Commerce export control regulations.

(14) *Information Exempt from the Requirement of a Munitions License.* Information that may be exported under the general exemptions in subsection 125.4 of ITAR.

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

(1) Training of foreign personnel, including visits directly related to training. (See AR 12–15.)

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

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

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

f. This regulation does not authorize, under any conditions, disclosure of the following:

(1) Classified information, the disclosure of which is prohibited by Federal Legislation; the Atomic Energy Act of 1954, as amended; or any international agreement to which the United States is a party.

(2) Proprietary information (for example, trade secrets), the rights to which are owned by private firms or citizens, without the owners' express written consent or other legal authorization.

(3) CMI or CUI without comments, recommendations, and concurrence of the proponent or originator of the information, as follows:

(a) Information acquired from a foreign government or international organization may not be disclosed to a third party without the written consent of the originator.

(b) Combined information (see glossary) may not be disclosed without the consent of all parties that contributed to the product.

(c) Joint information (see glossary) may not be disclosed without prior agreement of all parties having jurisdiction.

(d) Information originated by an agency outside DA may not be disclosed without the consent of the originator. For intelligence information, DoDD C–5230.23 and AR 381–1 must be complied with.

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

Section II
Responsibilities

1–6. HQDA Deputy Chief of Staff for Intelligence (DCSINT)

The HQDA DCSINT will—

a. Formulate Army policies governing contact with and disclosure of information and technical data to foreign representatives and provide general guidance, advice, and assistance to DA officials determining the suitability of CMI and CUI for foreign disclosure. Such action will be in accordance with the NDP–1, DODD 5230.11, DODD 5230.20, DODD 5230.24, DODD 5230.25, DODD 5400.7, and DOD 5200.1–R. The DCSINT will—

(1) Exercise exclusive approval authority for disclosure of official Army information, both classified and controlled unclassified, to foreign representatives (foreign disclosure). The ODCSINT, DA may specifically delegate authority to DA subordinate elements (MACOMs and below).

(2) Exercise approval authority for visits by foreign representatives and certification of foreign liaison officers and exchange personnel to DA elements. The ODCSINT, DA may specifically delegate authority to DA subordinate elements to approve visits.

b. Provide an Army member to represent the Secretary of the Army to the following:

(1) National Disclosure Policy Committee (NDPC).

(2) DoD International Technology Transfer Panel.

c. Control internal distribution of NDP–1 and provide necessary delegated disclosure authority to implement NDPC Records of Action throughout DA.

d. Provide overall direction to Army technology security program and be the primary point of contact (POC) for technology transfer issues on the Army Staff. In this role, the DCSINT will—

(1) Task the U.S. Army Materiel Command (AMC) to prepare technical assessments, as needed, identify militarily critical technologies, and provide additional technical support for technology transfer issues.

(2) Task specific agencies to conduct intelligence, counterintelligence, and operations security (OPSEC) assessments, as appropriate, of technologies and systems proposed for transfer.

(3) Provide staff review of all Army actions with technology security implications.

(4) Ensure that technology security is considered for each program that potentially involves the international transfer of CMI and CUI.

(5) Chair the Technology Control Panel (TCP) as a coordinating mechanism for technology security.

(6) Determine if counterintelligence or OPSEC safeguards can be devised to preclude diversion of critical technology associated with any proposed transfer.

e. Ensure that decisions to disclose or deny CMI or deny CUI are recorded in the Foreign Disclosure Technical Information System (FORDTIS) in compliance with DOD Instruction (DODI) 5230.18.

f. Record decisions on foreign visits to DA elements involving access to CMI or CUI, and liaison officer and exchange personnel certifications in the Foreign Visits System (FVS) in compliance with DODI 5230.18.

g. Conduct periodic on-site visits to organizations, agencies, activities, installations, and facilities over which DA exercises administrative control or security cognizance, to ensure compliance with this regulation.

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

Heads of HQDA staff agencies and MACOM Commanders will—

a. Ensure that their personnel follow the provisions of this regulation, and any additional instructions, when interacting with visiting foreign representatives, liaison officers, and exchange personnel.

b. Designate, in writing for each HQDA section, agency, or MACOM, a single official to be the Foreign Disclosure Officer (FDO). The FDO will exercise the organization's disclosure authority.

c. Publish agency or MACOM instructions that will ensure that—

(1) All CMI and CUI being considered for foreign disclosure are referred to the Foreign Disclosure Officer (FDO) for appropriate coordination. Final foreign disclosure decision will be in compliance with NDP–1.

(2) Agency and command personnel release no CMI or CUI to foreign representatives, other than those authorized by this regulation.

(3) Proposed foreign disclosures of CMI and CUI are considered in light of disclosure criteria prescribed in this regulation.

(4) Decisions to disclose or deny CMI and denials of CUI are recorded in FORDTIS, in accordance with DODI 5230.18.

d. Obtain concurrence of the ODCSINT, DA before implementing policies that involve disclosure of CMI or CUI to visiting foreign representatives, liaison officers, or exchange personnel.

e. Provide support to the Army technology security program.

f. Identify critical technology incorporated into systems and data they manage and with intelligence support assess the impact of compromise on those systems.

g. Take final action on routine technology transfer decisions.

h. Process violations of policies and procedures contained in this regulation in the manner prescribed either for compromise of CMI, as provided in AR 380–5, chapter 6, or for unauthorized disclosure of CUI outside the U.S. Government, as provided in AR 70–31, AR 25–55, and the ITAR.

1–8. HQDA Deputy Chief of Staff for Logistics (DCSLOG)

The HQDA DCSLOG will—

a. Assess implications of proposed transfers of critical technology on HQDA DCSLOG's programs, plans, and policies.

b. Verify that proposed transfers of critical technology are consistent with security assistance policy.

c. Coordinate and disseminate ARSTAF policy position on munitions export license requests for both munitions list and dual use systems and technologies.

d. Ensure that technology security implications are considered for each program for which the HQDA DCSLOG has primary ARSTAF responsibility and which potentially involves the international transfer of critical military technology.

e. Determine if the proposed transfer is consistent with previous export license application review decisions and FMS cases. The HQDA DCSLOG will ensure that adequate justification is provided for cases that are not consistent with previous Army positions.

f. Determine whether adequate technical and contractual safeguards can be, or have been, devised to preclude the diversion of critical technology.

g. Initiate requests for Exception to National Disclosure Policy in support of security assistance programs and direct commercial sales.

h. Formulate, coordinate, and disseminate weapon systems export policy.

i. Review and coordinate on Technology Assessment control Plans, DDLs and other documents that affect the sale/transfer of equipment and information via FMS or direct commercial sales.

j. Provide a representative to the TCP.

k. Designate an official POC to represent the HQDA DCSLOG on all international technology transfer actions.

1–9. HQDA Deputy Chief of Staff for Operations and Plans (DCSOPS)

The HQDA DCSOPS will—

a. Assess political and military factors of proposed transfers in accordance with criteria listed in figure 1-1 and make recommendations based on an evaluation of whether potential political and military gains outweigh the risk of loss if the transfer is approved.

b. Assess operational impact on U.S. forces if the transfer is approved and the technology or end item is transferred directly or indirectly to a potential U.S. adversary.

c. Ensure that technology security implications are considered for each program for which DCSOPS has primary ARSTAF responsibility, and which potentially involves the international transfer of CMI or CUI.

d. Assess implications of proposed transfers on DCSOPS programs, plans, and policies.

e. Provide a representative to the TCP.

f. Designate an official POC to represent the DCSOPS on all technology transfer issues.

g. Assess whether follow-on requirements, such as training, associated with the proposed transfer would involve the release of critical technology.

h. Administer, manage, and execute the U.S. Army Personnel Exchange Program with Armies of Other Nations (PEP). (See AR 614–10.)

1–10. Assistant Secretary of the Army (Research, Development and Acquisition)(ASA(RDA))

The ASA(RDA) will—

a. Identify critical technologies and items that should not be transferred to foreign entities.

b. Validate technology assessments and Technology Assessment/Control Plans (TA/CPs).

c. Assist in review of munitions export licenses referred to the ARSTAF for policy determination in accordance with the criteria set forth in AR 12–8.

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

e. Identify and assess applied and emerging militarily critical technologies.

f. Provide direct staff support to the Army member of DOD International Technology Transfer Subpanel B (Research and Development (R&D)).

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

h. With the HQDA DCSLOG and The Judge Advocate General (TJAG), devise effective technical and contractual safeguards to prevent the diversion of critical technology.

i. Assess whether continuing requirements associated with the proposed transfer also would involve the release of other technologies.

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

k. Provide a representative to the TCP.

l. Designate an official POC to represent the ASA(RDA) on all technology transfer issues.

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

CG, INSCOM will—

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

b. Provide a representative as an observer to the TCP.

c. Provide SAEDA special briefings, as specified in paragraph 2–3 of AR 381–12, to DA agencies and commands hosting foreign visitors, scientist and engineer exchange personnel, liaison officers, and students. Debrief those Army personnel having contact with foreign visitors and exchange personnel, when appropriate.

d. Provide tailored multi-disciplined counterintelligence threat briefings for technologies subject to technology transfer and to agencies and commands hosting foreign representatives.

e. Conduct counterintelligence investigations into incidents of illegal diversion of militarily critical Army technology in accordance with the provisions of AR 381–47.

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

The CG, AMC is responsible, in accordance with Army policy guidelines provided by the HQDA DCSINT, for the execution of the Army's Technology Security Program. CG, AMC may delegate authority within the framework of Army Regulations to accomplish the spirit and purpose of international technology transfer control. Specifically, the CG, AMC will—

a. Designate a single POC for technology security in Headquarters (HQ), AMC.

b. Develop assessments to identify militarily critical technologies or emerging technologies required for development, production, or operation of U.S. Army systems; and identify and provide an assessment of relative risks and benefits of international cooperation and technology transfer in those technologies.

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

d. As directed by and in coordination with HQDA, assess whether effective technical and contractual safeguards can be devised to preclude diversion of critical technology in conjunction with any proposed transfer.

e. At ASA(RDA) direction, provide technical experts to participate in Coordinating Committee for Multilateral Export Controls (COCOM) list reviews as required and ensure that the opinions rendered by those experts accurately reflect the Army position on any given technology.

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

g. As directed by HQDA, provide continuing assessment of control and transfer mechanisms and their effectiveness.

h. Coordinate intelligence assessments for all international cooperative programs.

i. Provide a representative to the TCP.

1–13. The Judge Advocate General (TJAG)

TJAG will—

a. Ensure that technology security implications are considered for each program for which TJAG has primary ARSTAF responsibility and which potentially involves the international transfer of CMI or CUI.

b. Together with HQDA DCSLOG and ASA(RDA), determine whether adequate technical and contractual safeguards can be developed to preclude the diversion of critical technology.

c. Provide a legal advisor to the Chairman of the DA TCP.

d. Provide direct staff support to the Army member of the DOD International Technology Transfer Panel and the NDPC.

e. Designate a lead POC to represent TJAG on technology transfer issues.

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

TSG, COE, and DISC4 will—

a. Ensure that technology security implications are considered for each program for which they have primary Army Staff responsibility and which potentially involves the international transfer of CMI or CUI.

b. Provide a representative to the DA TCP.

1–15. Directors and Commanders of Army Laboratories, R&D Centers, and Other R&D Activities

Directors and commanders of Army laboratories, R&D centers, and other R&D activities are responsible for carrying out the provisions of this regulation that directly pertain to their activities.

1–16. CG, U.S. Army Criminal Investigation Command (USACIDC)

The CG, USACIDC is responsible for the conduct of felony criminal investigations that involve technology transfer issues. CG, USACIDC will—

a. Investigate export violations as detailed in section 2410, title 50, United States Code (50 USC 2410), in accordance with 50 USC 2411.

b. Provide copies of final reports to HQDA DCSINT of investigations concerning illegal transfer of CMI or CUI.

c. Serve as POC to coordinate with the U.S. Customs Service and Department of State concerning enforcement of technology transfer issues.

d. Provide a representative as an observer to the TCP.

1–17. Overseas major commanders

Overseas major commanders are to use the policy guidance contained in this regulation to establish local policies and procedures governing interaction with foreign representatives. One copy of these policies and procedures will be forwarded to ODCSINT, DA (DAMI–CIT). For this purpose, overseas major commanders are U.S. Army Europe; U.S. Army Pacific; U.S. Army Southern Command; and Eighth U.S. Army. Army overseas major command components of unified commands are to adhere to unified command policies and procedures if only minor variances exists. ODCSINT, DA (DAMI–CIT) will be advised of conflicts. Significant conflicts will be resolved at the DA/DOD level.

1–18. Other Overseas Army Activities

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

Section III
Categorization, Disclosure and Funding Procedures

1–19. Categorization of Military Information by Sensitivity

a. CMI is information that 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. (See AR 380–5 for details regarding the classification of defense information.)

(1) According to its degree of sensitivity, CMI is identified by a level of security classification: CONFIDENTIAL, SECRET, or TOP SECRET.

(2) Certain CMI may be further protected, and, in some instances, access to it may be subject to greater limitation by the addition of annotations (caveats) restricting dissemination, as prescribed in various Army regulations (such as AR 380–5 and AR 381–1).

b. Unclassified information is information that competent authority has determined not to require the degree of protection afforded by the application of a security classification. Nevertheless, certain unclassified information may be of such sensitivity as to warrant placing a degree of control over its use and dissemination—to further various national interests—whereas other unclassified information may not warrant any control over its dissemination.

(1) For the purpose of this regulation, the former kind of unclassified information is termed CUI and generally is consigned to one or more of the following categories:

(a) Information subject to the Privacy Act of 1974 or otherwise exempt from mandatory disclosure outside the U.S. Government under AR 25–55. Such information ordinarily qualifies for application of the protective marking FOR OFFICIAL USE ONLY.

(b) Technical information that relates to research, development, engineering, test, evaluation, production, operation, maintenance, or employment of military equipment systems and that, if disseminated outside the U.S. Government, would be subject to export controls prescribed in the Arms Export Control Act (AECA) (PL 90–629) or Executive Order 12470 (extension of the Export Administration Act, PL 96–72). Dissemination restriction notices to be placed on such information are contained in AR 70–11 and AR 70–31 (for technical and materiel-related information) and in AR 25–30 (for non-materiel-related information).

(c) Information deemed to be sensitive from the standpoint of operations security (OPSEC) (see AR 530-1).

(2) For the purpose of this regulation, unclassified information that does not qualify for the status of CUI—as described in b(1) above—is deemed to be actually or potentially in the public domain, that is, suitable for release to the public at large. "The public at large" encompasses not only citizens of the United States and immigrant aliens, but also citizens of all foreign countries, when such persons are acting in a private capacity. As noted throughout this regulation, only unclassified information in the public domain may be released to foreign personnel acting in a private capacity. Any requests for DA information received from foreign personnel acting in a private capacity will be handled as follows:

(a) Requests for CMI or CUI will be referred to the FDO. Such requests will be responded to with an explanation that such information is not available for release consideration on other than an official government-to-government basis; the requester's military attache based in the continental United States (CONUS) may make queries on behalf of the requester.

(b) Requests for information clearly in the public domain (such as, public affairs-originated publications, reprints of articles that were written by DA authors and have appeared in any public media) may be fulfilled at the discretion of the agency public affairs office.

1–20. Categorization of military information by nature and type

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

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

(1) *Category 1 - Organization, Training, and Employment of Military Forces.* Information of a general nature pertaining to tactics, techniques, tactical doctrine and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for operation, training and maintenance on specific equipment covered under categories 2 and 3.

(2) *Category 2 - Military Materiel and Munitions.* Information on specific items of equipment already in production, or in service, and the information necessary for operation, maintenance and training. Items on the US Munitions List fall within this category. This category does not pertain to equipment which is in research and development.

(3) *Category 3 - Applied Research and Development Information and Materiel.* Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.

(4) *Category 4 - Production Information.* Designs, drawings, chemical, and mathematical equations, specifications, models, manufacturing techniques, software source code, and related related information (excluding Category 2 and 3 information) necessary to manufacture military materiel and munitions.

(5) *Category 5 - Combined Military Operations, Planning and Readiness.* 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. It does not include Strategic Plans and Guidance or North American Defense Information.

(6) *Category 6 - U.S. Order of Battle Information pertaining to U.S. forces in a specific area.* In general, disclosures of this information are limited to those countries in which US forces are stationed or are in adjacent geographical areas.

(7) *Category 7 - North American Defense.* Information related to plans, operations programs and projects, in include data and equipment, directly related to North American defense.

(8) *Category 8 - Military Intelligence.* Information of a military character pertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence.

1–21. Designated disclosure channels

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. All requests for foreign disclosure, irrespective of point of receipt within DA, will be referred through command foreign disclosure channels to the HQDA staff agency or MACOM exercising applicable disclosure authority, as provided in paragraph 2–11, below. MACOM subordinate or interested HQDA agencies will coordinate their positions on release of specific information before submission to the decision authority for a formal position.

b. Disclosure determinations are to be made at the lowest level consistent with the disclosure authority delegated in paragraph 2–11, below.

c. Similarly, requests for foreign disclosure relating to U.S. research, development, and acquisition (RD&A) initiatives are to be responded to by the DA agencies or commands exercising disclosure authority over the information requested for release. DA agencies and commands are encouraged to effect coordination with non-DA agencies when required. Should problems arise during the coordination process outside of DA, the request will be forwarded through local foreign disclosure channels to ODCSINT, DA (DAMI–CIT) for resolution.

d. ODCSINT, DA, is to receive and respond to foreign disclosure requests, except as follows:

(1) A request by a foreign representative during an approved visit is to be addressed by the designated DA host (see para 4–2).

(2) A request by a certified foreign liaison officer (LNO) is to be addressed directly to the DA agency or command to which the officer is certified. That agency or command will render a response (see para 4–4).

(3) A request by a certified British, Canadian, or Australian standardization representative is to be addressed directly to the DA agency or command to which the representative is certified. The agency or command will render a direct response in the case of information on projects listed on the ABCA standardization list and determined to be releasable under the provisions of this regulation. Requests for information for which the command is not the sole proponent will be fully coordinated with all concerned agencies. Denials will be referred to the ABCA Standardization Office located within HQ AMC for resolution in accordance with AR 34–1.

(4) Requests relating to acquisition of defense articles and services through security assistance channels (see para 4–7).

(5) Requests rendered in channels specified in certain approved international cooperative R&D agreements (Mutual Weapons Development Data Exchange Program (MWDDEP) or Defense Development Exchange Program (DDEP) agreements in accordance with AR 70–33).

(6) Requests addressed to outside continental United States (OCONUS) MACOM components of unified commands in channels specified in certain international agreements providing for combined planning and operations.

e. Any request that involves the potential foreign release of DA CMI or CUI and is received by a DA agency or command in a manner other than that prescribed by applicable DOD and DA regulations is to be routed to the appropriate DA disclosure authority if possible. If the appropriate DA disclosure authority cannot be determined, the request will be referred in command foreign disclosure channels to ODCSINT, DA (DAMI–CIT) for resolution.

1–22. Security protection and assurances

A foreign government or international organization is not to be provided U.S. CMI or CUI unless it has formally agreed to afford such information a degree of protection equal to that afforded by the U.S. Government. To that end, the Departments of State and Defense have concluded bilateral General Security of Military Information Agreements (GSOMIAs), which incorporate the conditions specified in paragraph 2–5, with various foreign governments and with NATO.

a. DA agencies or commands negotiating international agreements under AR 550–51, if the agreements potentially involve CMI or CUI, must ensure that such agreements address the issue of security protection to be afforded such information.

(1) For agreements negotiated with foreign governments and international organizations that are parties to existing GSOMIAs, the security provisions specified in the GSOMIAs will be incorporated in the agreements.

(2) All other agreements are to incorporate those provisions in either the text of the agreement or an internally referenced appendix.

b. GSOMIAs are accepted as agreements in principle only. Each individual transaction requesting the release of CMI or CUI must include a statement of security assurance recognizing the foreign government's responsibility and intent to comply with U.S. Government's security requirements. Such transactions include foreign organizations' requests for visits, certification, and documents.

c. In exceptional circumstances, fulfillment of U.S. interests may require disclosure of CMI or CUI to foreign elements without a formal agreement providing for adequate security protection. A disclosure of this nature may be authorized by ODCSINT, DA after appropriate coordination with national agencies having a direct interest in the disclosure.

d. Except as noted in c above, Army personnel should report unauthorized disclosures of CMI or CUI to ODCSINT, DA (DAMI–CIT) through command security or foreign disclosure channels.

1–23. Security Classification Guidance for DA Foreign Disclosure Activities

Table 1–1 is a security classification guide pertaining to routine foreign disclosure activities. Any related activity not addressed in table 1–1 is to be brought to the attention of ODCSINT, DA (DAMI–CIT) for resolution and in the interim is to be treated as CONFIDENTIAL, citing this paragraph as classification authority.

1–24. Nature of contacts with foreign representatives

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 U.S. Government prescribe that disclosed information must be suitable for release to the public or to another governmental entity in furtherance of a legitimate U.S. Government purpose. This regulation presumes that all contacts initiated by foreign representatives with other than public affairs elements of the Army are for the exchange of official information and must be legitimate government-to-government or authorized commercial exchanges.

1–25. Channels of official communication

a. On behalf of the Secretary of the Army and the Chief of Staff, the HQDA DCSINT or designee is the exclusive DA POC for military attaches diplomatically accredited to the U.S. Government and other representatives of foreign governments wishing to conduct official business with DA. All official foreign contacts with the Army must be requested by diplomatically accredited military attaches on behalf of their government. Foreign military attaches are provided with a handbook summarizing policies and procedures contained in this regulation.

b. Except as authorized by the HQDA DCSINT or senior Army leadership (Secretary of the Army, Under Secretary of the Army, Chief of Staff, or Vice Chief of Staff), foreign representatives are not authorized official contact or communications with either DA personnel or DA organizations in any manner pertaining to 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 ODCSINT, DA by their respective military attaches. Except as required by AR 381–12, no report to ODCSINT, DA of such unauthorized contact is necessary.

1–26. Funding and other support rendered to foreign representatives

Except when consistent with Federal statutory authority and specifically authorized by approved international agreements or in other Army regulations, no DA funds or other resources may be used to support the activities of foreign representatives while visiting or certified to DA. Military attaches are informed that they must be prepared to defray all costs incurred as a consequence of visits or certification to DA; however, to the extent authorized by applicable international agreements and Army regulations, local commanders may provide limited support (such as, medical care under AR 40–3; transportation aboard Army aircraft under AR 95–1; housing under certain circumstances under AR 210–50).

Table 1–1
Security Classification Guide for Disclosure-Related Activities

Subject Matter	Classification	Remarks
A. The Charts in Annex A of NDP–1.	SECRET	
1. The permissive disclosure category entries for a foreign government or international organization.	CONFIDENTIAL	
2. Any comparison of the permissive disclosure levels of two or more foreign governments or international orgainizations.	SECRET	
B. The fact that a specific foreign country or international organization has agreed to afford US CMI and CUI the same degree of protection as afforded by the US Government.	UNCLASSIFIED	Unless the mere existence of the governing security agreement is classified, in which case the same classification applies.
C. Disclosure authority (as reflected in para 2–10 and 2–11).	UNCLASSIFIED	
D. Disclosure criteria (as reflected in para 2–4), without reference to a specific case, foreign government, or international organization.	UNCLASSIFIED	
E. Disclosure criteria for military intelligence as reflected in para 2–4 and AR 381–1.	CONFIDENTIAL	
F. Disclosure conditions for CMI (as reflected in para 2–5).	UNCLASSIFIED	
G. NDPC organization and membership.	UNCLASSIFIED	
H. NDPC procedures.	UNCLASSIFIED	Except for section IV.2.b, which is CONFIDENTIAL.
I. Specific disclosure policy pertaining to a specific foreign government or international organization, beyond information from the charts in NDP–1, annex A.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman, NDPC, when circumstances warrant.
J. Specific disclosure policy for selected weapon systems, equipment, and technologies.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman, NDPC, when circumstances warrant.
K. Information revealing the security policies, procedures, methods, or practices of a foreign country or international organization for protecting classified military information compiled by an NDPC Security Survey Team.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman, NDPC, when circumstances warrant.
L. Assessments, including deficiencies or recommendations, compiled by an NDPC Security Survey Team that would not result in adverse effects on foreign relations if disclosed but that could result in damage to the national defense if disclosed. For example, the deficiency concerns an exploitable vulnerability that, if revealed, could cause direct or immediate jeopardy to the security of US classified information.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman, NDPC, when circumstances warrant.
M. Deficiencies or recommendations compiled by the NDPC Security Survey Team that could result in adverse effects on foreign relations if disclosed.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman, NDPC, when circumstances warrant.
N. The above items shall be declassified on "OADR."		

Chapter 2
General Disclosure Policies, Authority to Disclose, and Delegation of Authority Introduction

Section I
Introduction

2–1. Concept

a. National security asset. Military information (as defined in the Glossary) is a national security asset or resource. It may be disclosed to foreign governments and international organizations only under certain conditions: First, the national security and other legitimate interests of the U.S. Government must be demonstrably furthered by doing so. Second, the information must be disclosed only on an authorized basis by U.S. Government officials designated for that purpose. Third, the country must be eligible for the information to be disclosed and the disclosure criteria and conditions of NDP–1 (listed in para 2–4 and 2–5 below) must be met.

b. Disclosure pursuant to International Agreements. U.S. participation in bilateral or multilateral agreements does not automatically authorize the disclosure of related CMI to other participants. It does not constitute an exemption from provisions of this regulation. Conversely, the lack of an international agreement does not always preclude disclosure. Each potential disclosure of CMI must be evaluated on its own merit. A disclosure determination must be made by designated disclosure authorities following criteria established in this regulation.

2–2. False impressions

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

2–3. Maximum classification disclosure levels

The NDPC has established maximum classification levels within each category of CMI which may be released to foreign governments or international organizations only by those individuals specifically designated to authorize disclosures by the head of their department or agency in NDP–1 (see chap 1). Maximum classification levels are depicted on charts in annex A of NDP–1.

a. To qualify for unilateral DA approval, CMI under consideration for foreign disclosure must not exceed the established maximum classification level for the nature of the information in question as outlined in NDP–1.

b. CMI falling beyond the maximum classification level may still be considered for disclosure if significant U.S. interests appear to warrant it. Basic disclosure criteria, conditions, and limitations in paragraphs 2–4, 2–5, and 2–6 below, must be fully satisfied. The HQDA staff agency or MACOM proposing or supporting disclosure of the CMI in question may propose an exception to the NDP–1.

c. Exceptions to NDP–1, other than those personally granted by the Secretary of Defense or Deputy Secretary of Defense, may be granted only by the NDPC. All Army requests for exceptions to policy will be forwarded through command channels to the HQDA functional area proponent for coordination and submission to ODCSINT, DA (DAMI–CIT). Sample format provided at appendix B.

2–4. Basic disclosure criteria

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

a. Disclosures in Categories 1 through 7 of chapter 1 will be made when all of the following criteria are satisfied—

(1) Disclosure is consistent with U.S. foreign policy and national security objectives concerning the recipient foreign government or international organization. For example:

(a) The recipient cooperates with the U.S. in pursuance of military and political objectives which are compatible with those of the U.S.

(b) A specific U.S. national purpose, diplomatic or military, will be served.

(c) The information will be used in support of mutual defense and security objectives.

(2) Disclosure is consistent with U.S. military and security objectives. For example:

(a) Disclosures of advanced technology, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology regardless of the intended recipient.

(b) The proposed disclosure reflects the need for striking a proper balance between pursuit of our mutual defense and foreign policy objectives on the one hand and the preservation of the security of our military secrets on the other.

(3) The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the U.S. The intent of a foreign government to protect U.S. classified military information is established in part by the negotiation of a GSOMIA or other similar security arrangement. Guidance in determining a foreign government's capability to protect U.S. information may be determined by an U.S. embassy security assessment, CIA risk assessment, or a NDPC security survey report.

(4) Disclosures will result in benefits to the United States 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 United States from a technical or other military viewpoint.

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

(5) The disclosure is limited to information necessary to the purpose for which disclosure is made.

b. Disclosures in Category 8 (Military Intelligence) will be made only when all of the following criteria are satisfied:

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

(2) Disclosure can be expected to result in a clearly identifiable advantage to the United States, such as—

(a) A specific U.S. national purpose—political, economic, or military—will be served.

(b) The U.S. will obtain commensurate information or services from the proposed recipient.

(c) The intelligence to be disclosed supports specific bilateral or multilateral plans, arrangements, treaties, or alliances. Formal intelligence agreements to support such arrangements will be approved in advance by the Director, DIA.

(d) An advantage will be gained for U.S. intelligence or counterintelligence operations.

(3) It can be reasonably presumed that the disclosed intelligence will not be used in a manner harmful to U.S. interests. In particular—

(a) The intelligence will not be disclosed to a third government or any other party without the approval of the releasing U.S. department or agency.

(b) The intelligence will be provided substantially the same degree of protection provided it by the United States. Guidance in determining a foreign government's ability to protect U.S. intelligence may be obtained from an embassy security assessment, CIA risk assessment, and a National Disclosure Policy Committee Security Survey Report.

(c) The intelligence will not be used for other than the stated purpose without the approval of the releasing department or agency.

(4) Specific disclosure criteria pertaining to individual countries is contained in NDP–1. Further, NDP–1, section II, contains a discussion of prohibitions or limitations in the release of intelligence information.

2–5. Disclosure conditions

After a decision is made to disclose classified military information to a foreign government or international organization based on the above listed criteria, or an exception to policy, release of the classified military information will be contingent upon assurances that the following minimum conditions will be met:

a. Security to be afforded by the recipient. Disclosures will not normally be made until the disclosure authority is in receipt of assurances from the recipient that—

(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 (each British Commonwealth nation should be treated separately).

(2) The information will be afforded substantially the same degree of security protection given to it by the U.S.

(3) The information will be used for specified military-related purposes only, including production for military use when so authorized.

(4) The recipient will report promptly and fully to U.S. authorities any known or suspected compromise of U.S. classified military information released to them.

(5) All individuals and facilities that will have access to the classified military information 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.

(6) The foreign recipient of the information has agreed to abide by or meet U.S.-specified special terms and conditions for the release of U.S. source information or materiel.

b. Specifically prohibited disclosures are as follows:

(1) Classified military information officially obtained from a foreign source, except when the information has been conveyed by the source with express consent to its further disclosure.

(2) Combined military information without prior agreement of all parties.

(3) Joint information without prior agreement of all departments or agencies having control or jurisdiction.

(4) Information originated by or for any department or agency, without its consent.

c. In documentary or materiel disclosures, a statement will be included in transmittal correspondence, contract or receipt, or affixed to the document itself indicating that the document or materiel is provided with the understanding that the recipient will comply with the listed conditions. When appropriate, a similar cautionary statement will be included in oral or visual disclosures.

2–6. Disclosure limitations

Potential foreign disclosures that are within established maximum classification levels (para 2–3) and meet all prescribed basic disclosure criteria (para 2–4) still must meet certain additional limitations. These limitations are essential to a foreign disclosure program that successfully promotes national security interests. Most of these limitations are related to disclosures of specific categories of information or are related to DA participation in specific types of international functions or agreements (see specific guidance in chap 3). The limitations below are general in scope. They apply to all disclosures of CMI and CUI.

a. DA CMI and CUI which relate to or contain critical technologies (see glossary) require additional evaluation under paragraph 2–8 here. DA officials considering this type of disclosure will ensure—

(1) A technical evaluation has been completed.

(2) The critical technologies have been identified.

b. Documentary information in draft form is not normally appropriate for disclosure. Normally, only the proponent exercising appropriate delegated disclosure authority will make the determination. Examples of such documentary materials are classified solicitations; operational test reports; conceptual studies; technical reports; materiel test and evaluation reports; and DA administrative, doctrinal, technical and training publications.

c. Bibliographic data (e.g. bibliographies, lists of references, bibliographic footnotes, literature surveys) must be considered for suitability for foreign disclosure. Such disclosures offer the potential for embarrassing misunderstanding or false impressions. The composite effects of test and related materials must be determined. Release of bibliographic references and footnotes to academic or technical papers is often essential in order to validate the thesis presented. To delete reference materials arbitrarily would lessen the quality of the product. Therefore, if release of the reference materials is considered inappropriate, the disclosure of the associated text may be inadvisable. Although security officers have responsibility to ensure compliance with this regulation, they often do not have the technical expertise to sanitize publications. The responsibility for deleting unreleasable information from a technical document lies with the proponent or, in the case of a cooperative agreement, the technical coordinator for the Memorandum of Understanding (MOU). The proponent or technical coordinator will certify to the security officer that the publication has been sanitized to the extent necessary or that all references should remain in the proposed document, less distribution lists.

2–7. Establishment of Disclosure Programs

a. An international or functional agreement that could reasonably be expected to lead to the release of CMI to foreign governments or international organizations constitutes one example of a "disclosure program." The agreement forms the substantive basis for future disclosure determinations.

b. To avoid giving the false impression that the DA may subsequently approve classified disclosures, certain actions must be taken. DA management officials responsible for reviewing, providing input, or negotiating a DA or higher level agreement must assure that the CMI disclosure implications of potential agreements are identified at the outset of the program. Such officials shall coordinate their activities with the local FDO in advance of a position, comment, or negotiation to insure the agreement fully conforms to the policies prescribed in this regulation.

c. The proposed 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 HQDA staff agency or MACOM at which the proposed agreement originates. It will be accomplished with the technical assistance of the agency or MACOM FDO. The FDO will ensure that the views of all interested parties (including the U.S. Defense Attache Office, USDAO, or other U.S. officials residing in and knowledgeable of the country(ies) to be party(ies) to the agreement) are obtained and incorporated.

(1) If the FDO concludes that only CUI will be disclosed, the FDO may concur in the start of negotiations.

(2) If the FDO concludes that CMI will or is likely to be disclosed, the FDO may concur in proceeding with negotiations only to the extent that potential CMI disclosures—

(a) Are referred to the primary disclosure authority identified in paragraph 2–11 for consideration. An action originating at the MACOM level that requires a decision from an HQDA primary disclosure authority will be referred through command foreign disclosure channels to HQDA for consideration by the primary disclosure authority. The primary disclosure authority will complete such coordination as may be necessary among other HQDA staff agencies before approving the disclosure program. If coordination with DOD or other Federal agencies is required, the primary disclosure authority will refer the action to ODCSINT, DA (DAMI–CIT). DAMI–CIT will effect necessary coordination and return the action to the DA originator. The DA primary disclosure authority will approve or deny the disclosure program and authorize subsequent CMI disclosure determinations to be made by DA officials accordingly. Primary disclosure authorities will comply with requirements to record disclosure decisions in FORDTIS as specified in paragraph 4–10.

(b) Do not exceed the maximum classification levels established by NDP–1 for the CMI Category(ies) involved. Caution must be exercised if an exception to NDP–1 is necessary. Only information up to the maximum classification level established may be disclosed in the absence of an approved exception to NDP–1.

(c) Do not exceed the authority delegated to the FDO's Agency or MACOM in paragraph 2–11. If they do, the FDO is to refer the matter to the primary delegated disclosure authority for the category of information involved. The primary delegated disclosure authority will act on the issue or refer it to ODCSINT, DA for disclosure determination.

2–8. International technology transfer policy

This section provides the basis for the Army Technology Security Program. It should be used in conjunction with the remaining sections of this regulation, as applicable.

a. Policy guidance.

(1) Militarily critical technologies and items of intrinsic military utility are valuable limited national security resources. They must be protected and used in a manner consistent with national security and foreign policy objectives. Consistent with this policy, and in recognition of the importance of international trade, the Army will apply technology security control in a way that minimally interferes with the conduct of legitimate trade and scientific endeavor. Therefore, Army components will—

(a) Manage international transfers of technology, goods, services, and munitions consistent with U.S. foreign policy and national security objectives.

(b) Control the release of technology, goods, services, and munitions that contribute to the military potential of any country or combination of countries that could prove detrimental to U.S. security interests.

(c) Limit the transfer of advanced design and manufacturing know-how regarding technology, goods, services, and munitions to

only those governments that support specific national security or foreign policy objectives.

(d) Facilitate the sharing of military technology with allies and other friendly nations that cooperate to safeguard technology, goods, services, and munitions.

(e) Give special attention to rapidly emerging and changing technologies to prevent militarily useful technology from being conveyed to adversaries before adequate safeguards can be implemented.

(f) Seek (through improved international cooperation) to strengthen foreign procedures for protecting sensitive and defense-related technology.

(g) Strive for reciprocity in every instance before transferring valuable defense-related technology.

(2) Public disclosure of technical data is tantamount to providing uncontrolled foreign access. Withholding technical data from public disclosure, unless approved, authorized, or licensed in accordance with export control laws, is necessary and in the national interest. Unclassified technical data which would disclose critical technology as defined by the Military Critical Technologies List (MCTL) are to be controlled under the provisions of this regulation and AR 70–31.

b. DA technology transfer decision criteria. All technology transfer decisions will be based on criteria listed in paragraph 2–4, above. The decision process for release of CUI is essentially the same as for disclosing CMI.

c. DA technology transfer decision process. DA technology transfer decision process is comprised of the elements listed below.

(1) Identification, with supporting rationale, of technologies and systems critically important to the Army, based on information from Army commands having materiel development responsibilities.

(2) Validated intelligence assessment to determine the value to adversaries of a given technology or system, and the risk of loss through diversion or other means if the proposed transfer is approved.

(3) Political-military, military-operational, economic, and other factors to determine impacts of transfer. This information will be developed by the HQDA DCSOPS based on criteria in figure 2–1.

(4) Determination as to whether or not potential benefits of the proposed transfer justify the risk.

d. Technology Transfer Decision Procedures. Authority for routine technology transfer decisions is delegated to MACOMs and may not be further delegated without prior written approval issued by ODCSINT, DA (DAMI–CIT).

(1) Decisions to permit technology transfer to foreign governments will be based on provisions of this regulation, NDP–1, applicable official international agreements, and criteria cited in paragraph 2–4, above.

(2) Decisions to deny transfer to foreign governments will be based on a determination that no official international agreement applies and that provisions of NDP–1 or MCTL guidelines would prohibit transfer. Decisions to deny transfer to foreign governments will be coordinated with ODCSINT, DA (DAMI–CIT) through command foreign disclosure channels.

e. Technology security document requirements. The following technology security documents are essential parts of the Army's Technology Security Program:

(1) *Technology Assessment/Control Plan (TA/CP).* Technology security elements identified in paragraph 2–8c, above, are vital elements of the TA/CP. The TA/CP is a DOD-mandated technology security document. It is required for all weapon systems where there is, or is a potential for, foreign participation. Development of TA/CP is the responsibility of the Program Manager (PM), in concert with appropriate international cooperative programs offices and foreign disclosure/security offices. In acquisition programs, TA/CP is a required annex to the Program Protection Plan (PPP). TA/CPs are also required as supporting documents for international agreements requiring OSD approval to negotiate or conclude. Format for a TA/CP is found at appendix C. Attached to each TA/CP is a Delegation of Disclosure Authority Letter (DDL) which describes scope and limitations about information that may be disclosed to specific foreign governments. The formats used for DDLs are at appendix D.

(2) *Program Protection Plan (PPP).* PPP also is a DOD-mandated document required only for acquisition programs. The purpose of the PPP is to identify essential program information, technology and systems to be protected and to create a management plan outlining the measures to be taken by the PM necessary to protect the weapon system throughout the acquisition process. The PPP is implemented by DODI 5000.2.

f. Technology Control Panel (TCP).

(1) In order to develop and manage Army technology transfer control policy for the DCSINT, the TCP was established. The Panel's mandate is to facilitate consistent and comprehensive technology transfer decisions based on thorough consideration of relevant factors. In addition, the TCP is tasked with resolving contentious or priority issues presented on a case-by-case basis, as deemed necessary by the TCP chair.

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

(a) Director of Counterintelligence-chair and DCSINT representative.

(b) Representatives from the following organizations; ASA(RDA), HQDA DCSLOG, HQDA DCSOPS, TSG, COE, AMC, TRADOC, USASSDC, and DISC4.

(3) TJAG will provide a legal advisor to the Chairman of the TCP.

(4) The following organizations will provide observers to the TCP as required: INSCOM, U.S. Army Security Assistance Command (USASAC), and U.S. Army Criminal Investigation Command (USACIDC).

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

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

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

(8) The TCP will meet quarterly at the call of the chair and on the request of one of the TCP members.

2–9. DA contractor functions

a. Export controls. DA contractors must follow the requirements of the ITAR, the Industrial Security Manual (ISM) (DOD 5220.22–M), and, where applicable, the EAR when the export or disclosure of classified or controlled unclassified information is proposed.

b. Defense Industrial Security Program. Contractors who have been granted a facility clearance and have signed a Security Agreement (DD Form 441) with the DOD must abide by requirements of the DOD's Defense Industrial Security Program (DISP) run by the Defense Investigative Service (DIS) to be eligible to receive classified information. DA contractors must follow all requirements of the ISM and any specific contractual security requirements when classified information is involved.

Section II
Authority to Disclose Classified Military Information (CMI) and Controlled Unclassified Information (CUI) and Delegation of Disclosure Authority

2–10. CUI Disclosure Authority and Delegation of Authority

Authority to approve or deny the disclosure of CUI to authorized foreign representatives is vested in the DA agency head or MACOM commander of the organization designated as the information proponent. The agency head or MACOM commander may

further delegate such authority to the lowest practical level consistent with good security practices. (The disclosure approval authority for information controlled under AR 70–31 and AR 25–30 is to be clearly identified on documentary materials containing the information.)

2–11. CMI disclosure authority and delegation of authority

On behalf of the Secretary of the Army, the HQDA DCSINT exercises exclusive authority to approve or deny disclosure of CMI originated by or for DA for which DA is the DOD component having primary substantive interest or which is otherwise determined to be under the security and disclosure cognizance of DA. The HQDA DCSINT has delegated portions of this authority to selected heads of HQDA staff agencies and MACOM commanders on a continuing basis. Periodically, the HQDA DCSINT may elect to delegate additional specific disclosure authority. Notice will be disseminated in the form of DDLs. Delegated disclosure authorities identified in this section may approve or deny the disclosure of CMI, but in each case this authority is limited to categories and eligibility levels cited. Approval of the primary delegated authority is always required.

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

(1) The Deputy Chief of Staff for Operations and Plans (DCSOPS), HQDA, is the primary delegated authority.

(2) The Director of Information Systems for Command, Control, Communications and Computer (DISC4), HQDA also has authority to make disclosure decisions for Category 1 CMI within the scope cited.

(3) The Commander, U.S. Army Training and Doctrine Command (TRADOC), has authority within the scope cited and also may approve disclosure of Category 1 CMI to fulfill foreign training requirements established under AR 12–8 and AR 12–15.

(4) TSG (DASG)/U.S. Army Medical Command (USAMEDCOM), has authority to make disclosure decisions for medical related Category 1 CMI within the scope cited and to fulfill foreign training requirements established under AR 12–8 and AR 12–15.

(5) The following officials have authority limited to NATO and its member nations, ABCA and its member nations, Japan, and the Republic of Korea:

(a) Commander, U.S. Army Information Systems Command (USAISC).

(b) Commander, Forces Command (FORSCOM).

(c) Commander, U.S. Army Intelligence and Security Command (INSCOM).

(d) Commanders, U.S. Army MACOM components of unified commands.

(6) The Commander, U.S. Army Space and Strategic Defense Command (USASSDC) has authority to make disclosure decisions regarding Categories 1 and 3 CMI to fulfill RSI requirements for the development of concepts and requirements data related to architecture and systems development studies for Army programs supporting the Ballistic Missile Defense Organization (BMDO).

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

(1) Deputy Chief of Staff for Logistics (DCSLOG), HQDA is the primary delegated authority.

(2) ASA(RDA) has authority concerning CMI related to adoption of materiel items for allied or friendly government RSI.

(3) Commander, U.S. Army Materiel Command (AMC), has authority within the scope cited as authorized by HQDA DCSLOG.

(4) Commander, U.S. Army Security Assistance Command (USASAC), has authority in keeping with the ODCSLOG-authorized disclosure authority.

(5) TSG (DASG), has authority concerning CMI related to security assistance associated medical materiel services.

(6) The following officials have authority limited to CMI pertaining to tactics and doctrinal techniques necessary to successfully use materiel items that are in the inventory of, or planned for sale to, the foreign governments that are the prospective recipients of the CMI:

(a) DCSOPS, HQDA.

(b) DISC4, HQDA.

(c) Commander, TRADOC.

(7) DCSOPS, DA also participates in the disclosure process for ABCA Primary Standardization Office and its member nations per its primary staff responsibility in that functional area.

(8) Commander, FORSCOM, has authority extending to items and materiel that are in U.S. Army inventories and are in use in overseas deployment during joint or combined exercises and operations. Disclosure may occur when RSI will be served best by oral or visual release of CMI to participating forces of allied or friendly governments.

c. Officials listed in the subparagraphs below have authority to make disclosure determinations for Category 3 CMI (Applied Research and Development Information and Materiel). This authority applies within the substantive scope of international cooperative R&D agreements approved under AR 70–33, AR 70–41, and AR 550–51 and pertains to information about developmental materiel items approved for allied and friendly government RSI.

(1) OASA(RDA) is the primary delegated authority.

(2) Commander, AMC, also has authority within the scope cited.

(3) Officials listed below have authority limited to CMI pertaining to projected tactics and doctrinal techniques for use of materiel items in the demonstration and validation or full-scale development phase. (See AR 70–1.)

(a) DCSOPS, HQDA.

(b) DISC4, HQDA.

(c) Commander, TRADOC.

(4) Commander, USASSDC, has authority limited to CMI pertaining to the Army's participation in the Ballistic Missile Defense Program and to related strategic and conventional applications of technologies identified by the BMDO.

(5) Commander, FORSCOM, has authority limited to CMI pertaining to Army development of tactical materiel and equipment particular to operational units. Coordination with Commander, AMC, for CMI inherent in developmental technologies, is required prior to exercise of disclosure authority.

d. Disclosure determinations concerning classified Category 4 CMI (Production Information) are accomplished by specific DDLs.

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

(1) DCSOPS, HQDA is the primary delegated authority.

(2) Commander, TRADOC.

(3) Commander, FORSCOM.

(4) Commanders of U.S. Army MACOM components of unified commands.

(5) Commander, USASSDC (authority pertains to U.S. Army efforts as well as Theater Missile Defense studies and systems).

(6) TSG/Commander USAMEDCOM has authority for medical related CMI within the scope cited.

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

(1) DCSOPS, HQDA is the primary delegated authority.

(2) Commander, FORSCOM (in connection with actual or overseas deployment of FORSCOM elements).

(3) Commander, INSCOM.

(4) Commander, USAISC.

(5) Commanders of U.S. Army MACOM components of unified commands.

g. Disclosure determinations for Category 7 CMI (North American Defense) are accomplished generally by specific DDLs. The exception is that determinations pertaining to the Ballistic Missile Defense Program are covered by authority of Commander, USASSDC, as noted in *c*(4) above.

h. Disclosure determinations for Category 8 CMI (Military Intelligence) are generally accomplished by specific DDL only. However, commanders of MACOM components of unified commands are authorized to release MACOM-generated intelligence in support of combined combat operations, provided eligibility and criteria requirements established in the NDP–1 are met.

i. Fully justified proposals regarding further delegation of disclosure authority will be submitted in command foreign disclosure channels to ODCSINT, DA (DAMI–CIT) via the HQDA staff element holding primary delegated authority. The latter will provide comments either supporting or refuting the justification for further delegation of disclosure authority and will recommend approval or denial of the proposal. On approval of the proposal, ODCSINT, DA will issue a DDL.

2–12. Authority to release CMI and CUI

DA officials authorized to approve the disclosure of CMI and CUI may also authorize its release. They may authorize release by other DA officials on either a case-by-case or a continuing basis. Release authorizations on a continuing basis involving CMI are to be made a matter of record. A copy will be furnished to ODCSINT, DA (DAMI–CIT). Designated channels for release are prescribed in paragraph 1–20, above and amplified in chapter 4.

2–13. Authority to deny foreign disclosure of CMI and CUI

DA officials authorized to approve the foreign disclosure of DA CMI and CUI are also authorized to deny such foreign disclosure. Designated DA officials are to ensure that denials are consistent with the policies prescribed herein. ODCSINT, DA (DAMI–CIT) must be advised of any denials of CMI or CUI.

Figure 2–1. Political and Military Criteria

Political considerations

a. The potential foreign recipient's support for US 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 US interests.
c. The effects of the regional and global strategic balance if the transfer is approved.
d. Whether or not the country has a defense treaty or political agreement with the United States.
e. The political benefits that could accrue to the United States.
f. Whether or not the transfer helps the United States to obtain or secure base, transit, and overflight rights or access to strategic locations.
g. Other countries to which the United States has transferred the item.
h. The possible reaction of other countries in the region to the proposed sale.
i. Whether or not the United States is the first supplier of the item.
j. The possibility that the item cound fall into the hands of terrorists.
k. The impact of the transfer on the country's economy.
l. Whether or not the transfer establishes an unfavorable political precedent.

Military considerations

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

Chapter 3
Policies and Procedures for Specific International Activities

Section I
Introduction

3–1. International activities (excluding security assistance actions) prompting CMI and CUI disclosures

a. The potential release 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 in accordance with AR 550–51. On approval, these agreements constitute disclosure programs and form the basis on which disclosure determinations may be made unilaterally by DA. The DDL, approved by ODCSINT, DA (DAMI–CIT), constitutes disclosure guidance for the international agreement. Such agreements also provide the legitimate basis for foreign disclosure of CUI which otherwise would not be deemed suitable for release outside the US Government.

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

c. The policies and procedures prescribed in this regulation are considered sufficient for disclosure decisions involving DA CMI and CUI. However, disclosure pertaining to foreign involvement in the materiel acquisition process is more complicated and warrants additional guidance in accordance with sections II and III.

3–2. Coordination of proposed disclosures

a. All information necessary to make a disclosure decision is not always readily available to the designated disclosure authority. The concurrence of the information proponent is required, and the proponent is frequently not the agency or MACOM exercising disclosure authority. Also, in highly technical areas detailed substantive

expertise is rarely found at the level where disclosure authority resides. Agencies or commands having a substantive interest in the matter requiring a disclosure decision must be allowed to comment and make recommendations. MACOMs and sub-MACOM elements will coordinate laterally with all DA agencies having an interest in the information to develop a fully staffed and coordinated MACOM or DA agency position.

b. Comments and recommendations on issues related to the disclosure of either CMI or CUI will address to the maximum extent possible—

(1) If and to what degree the disclosure request satisfies each of the basic disclosure criteria in paragraph 2–4.

(2) If the information has previously been approved for disclosure to the foreign government in question and, if so, when, by whom, and in what form or context.

(3) If previous interaction with the foreign government in question indicates it possesses the technical capacity and expertise to use the information effectively.

(4) If the information contains or constitutes technical data or technical information (see definition in glossary). If so, the comments should describe the type and extent of critical technology included. If the disclosure would constitute a risk to the U.S. technological lead time, the comments should compare the information being considered for disclosure with current state-of-the-art.

(5) How approval of the disclosure in question would affect current or projected DA activities.

(6) If the information being considered for disclosure includes or pertains to any of the types of information cited in paragraphs 1–1e, f, and g. If so, the comments must clearly state the type of information and identify which portions of the information being considered for disclosure are involved.

(7) If the information falls within the substantive scope of an existing international or functional agreement which the recipient government has signed. If it does, the following must be identified: NATO panel or working group designator; ABCA working group, special working party or standardization list designator; Data Exchange Agreement (DEA); or, MOU or other agreement by title and date. Disclosure decisions will not always be predicated on a particular nation's participation in an international or functional agreement. Foreign industrial concerns wishing to compete with US industry for classified contracts present a unique situation. Disclosure authorities at all levels will consider the potential requirement for foreign participation and ensure that timely disclosure decisions are made.

(8) If similar information at a lower classification level would largely satisfy the disclosure requirement being considered. If so, the comments should identify fully the benefits to the US Army of disclosing information classified at a higher level.

(9) If the issue requires substantive coordination with other DA agencies. If so, correspondence reflecting such coordination should be attached.

(10) If the issue has been identified at the Army leadership level as having special interest for or against multinational participation. Has the Army Acquisition Executive identified the issue as one requiring special coordination action at HQDA over and above Army Staff (ARSTAF) review?

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

(12) What the recommended disposition of the issue is (for example, approve, approve with conditions, or deny). A brief rationale supporting the recommendation will be provided.

c. ODCSINT, DA (DAMI–CIT) may establish channels for coordination on routine matters to expedite the decision process. The integrity of the command foreign disclosure process will generally be followed. ODCSINT will provide results of its coordination to the DA agency or command that would otherwise exercise disclosure authority.

Section II
Security Assistance-related Disclosure of CMI and CUI

3–3. Concept

a. This section covers the disclosure and release of CMI and CUI 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, direct sale basis. Transfer means the sale, lease or loan, grant co-production, or reciprocal use. The transfer must be accomplished per agreements created under AR 12–1 and AR 12–8.

b. When a transfer will involve the disclosure of CMI, agreements leading to transfer must be coordinated and approved in the manner prescribed in paragraph 2–7. Such agreements principally involve the disclosure of information in Category 2, 4, and 8. In all cases, potential security assistance agreements will be coordinated with ODCSINT, DA (DAMI–CIT) prior to final approval.

c. In a security assistance context this 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 prescribed in AR 12–8. It may also be initiated unilaterally by DA or DOD in anticipation of potential sales or transfers as a result of a foreign government's request or a license application through the Department of State (DOS) (required for a direct commercial sale).

d. In keeping with NDP–1, the transfer of a single materiel item to a foreign government or international organization is normally prohibited. An exception may be made under certain conditions, such as if the prospective recipient would reasonably require no more than one in its inventory. An exception for leases or loans for the purpose of test and evaluation is discussed in paragraph 3–6.

e. 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 release. A technical data package (see definition in glossary) shall only be disclosed in accordance with procedures explained in paragraphs 3–4 *c* and *d*.

3–4. Disclosure of CMI and CUI on a security assistance basis

a. Pending HQDA determination of willingness to sell or otherwise transfer the materiel in question to a specific foreign government or international organizations—

(1) No CMI (irrespective of category) related to the materiel may be approved for disclosure.

(2) CUI (not including critical technology)—

(a) May be approved for disclosure if the potential sale or transfer could be accomplished without an exception to the NDP–1. Information disclosed must be accompanied by an express stipulation that this action is not to be construed as a U.S. Government commitment to sell or transfer the materiel or provide further related information.

(b) May not be approved for disclosure if subsequent sale or transfer of CMI would require an exception to NDP–1. This proscription prevents a false impression of the willingness of the US Government to participate in future transfers.

(3) Unclassified information that has been approved for release to the public under AR 70–31 and AR 360–5 may be provided to any foreign requester. However, each such release is to be accompanied by the stipulation in (2) *(a)* above.

b. If HQDA decides against the sale or transfer of the material in question, disclosure of information to the particular foreign government or international organization will be limited to that in *a*(3) above.

c. If HQDA decides to sell or transfer the materiel in question, delegated disclosure authorities may approve disclosure of CMI and CUI to the prospective recipient as follows:

(1) Prior to formal acceptance of the USALO (United States of America Letter of Offer and Acceptance) 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. No specific information on system countermeasures susceptibilities or vulnerabilities or countermeasures capabilities may be disclosed until the sale is consummated.

(a) The information specified in *c*(1) above is deemed essential and sufficient for the foreign government to make an informed judgement regarding potential acquisition. It may be exceeded only on approval by HQDA (DALO–SAC), following appropriate coordination.

(b) CMI or CUI approved for disclosure, but released in any manner other than with issuance of an LOA or letter of instruction, will be accompanied by the stipulation in *a*(2)*(a)*, above.

(2) After a foreign recipient has formally accepted an LOA, disclosures may be approved to the limit of the Army's delegated disclosure authority for the country as stipulated in NDP–1 for Category 2 information. The CMI or CUI disclosure must be directly related to the designated item approved for sale. Subsequent requirements for CMI and CUI pertaining to reliability, availability, maintainability and safety of the item may be approved for disclosure by designated DA officials on the basis of the original HQDA authorization for sale. This does not necessarily include CMI or CUI that would significantly improve the item's or system's performance or decrease its vulnerability to countermeasures, or allow release of classified production information pertaining to the item.

d. Proposed disclosure of other categories of CMI and CUI in relation to an agreement providing for the sale or transfer of U.S.-produced end items in security assistance channels will be governed as follows:

(1) Disclosure of Category 4 CMI is prohibited except with an approved exception to the National Disclosure Policy and following the implementation of an LOA for the information or as may be authorized by ODCSINT, DA (DAMI–CIT), with the concurrence of OASA(RDA) and ODCSLOG, DA.

(2) Disclosure of Categories 7 and 8 CMI and CUI is prohibited, except as may be specifically authorized by ODCSINT, DA (DAMI–CIT) and paragraph 2–11.

3–5. Disclosure of CMI and CUI on a licensed commercial basis

a. Mutual security assistance interests of the United States and foreign governments may at times be served better by the transfer of defense articles or services on a direct commercial sale basis (under AR 12–8). All initiatives involving defense articles and services are subject to munitions licensing prescribed by the DOS International Traffic in Arms Regulation (ITAR), implementing the AECA.

b. Overall DA policies and procedures governing the processing of munitions license applications are contained in AR 12–8. From the standpoint of approving the disclosure of CMI, processing such a license application constitutes a determination of willingness to sell and is subject to the disclosure-related restrictions prescribed in paragraph 2–6 and 2–7.

c. Processing and deciding on a munitions license application has very direct implications on potential commercial arrangements between US companies and foreign representatives. In the absence of an approved license or a pre-license "advisory opinion", the AECA/ITAR prohibits discussions among U.S. commercial and foreign representatives pertaining to defense articles and services. Exceptions are allowed if discussions involve information in the public domain or authorized by DOD. (See para 2–4 and 5–17 *f*, for explanation of the interrelationship of DOD, US companies, and foreign representatives.) Additionally, the existence of an approved munitions license can have direct implications for the disclosure of CMI and CUI by DA elements in their direct interaction with foreign representatives. DA elements must strictly adhere to disclosure guidelines to preclude circumvention of the licensing controls established by the AECA/ITAR.

(1) Pending issuance of an approved munitions license, the restrictions described in paragraph 3–4 *a* are applicable. The restrictions are consistent with AECA/ITAR restrictions imposed on US commercial firms.

(2) The denial of a munitions license may or may not constitute a negative determination of US willingness to sell. In some cases, licenses may be denied in favor of sale or transfer on a government-to-government basis.

(3) The approval of a munitions license authorizes the US commercial firm and the foreign government or international organization to proceed with negotiations toward, or the execution of, a possible sale or transfer. The restrictions on disclosure of CMI, described in paragraph 3–4a, are applicable to both the U.S. commercial firm and DA elements.

d. Data regarding the status of and substantive details pertaining to munitions license applications processed by DA and DOD are reflected in the FORDTIS. The DA Agency or MACOM FDO must obtain and incorporate such data when making disclosure determinations in the course of participation in other international activities. These determinations may only indirectly relate to the sale or transfer of defense articles or services (such as, disclosures to foreign visitors and certified LNOs).

3–6. Foreign test and evaluation of materiel

Administrative and operational requirements and restrictions governing the foreign test and evaluation of U.S. materiel are prescribed in AR 34–1.

a. Foreign test and evaluation of DA classified equipment may be authorized 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 or unclassified critical technology.

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

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

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

(3) The release will result in a clearly defined advantage to the United States. Examples are outlined below.

(a) Specifically defined avoidance of significant costs or acceleration of programs in development efforts by the United States and its allies.

(b) Advancement of objectives of standardization with and among US allies by promoting cooperation in R&D.

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

(4) The Secretary of the Army, in coordination with the Office of the Under Secretary of Defense for Acquisition, approves the exception as meeting the above criteria. The Chairman, NDPC, will be informed of each exception; the Chairman will in turn notify members of the NDPC.

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

(6) Proposals to authorize foreign test and evaluation in this manner, including reciprocal use loans of materiel under the auspices of NATO and ABCA standardization (see AR 34–1), will be submitted to OASA(RDA), who will—

(a) Coordinate with counterpart elements of the Air Force and Navy, depending on their interest in items or technologies associated with the information proposed for release.

(b) Coordinate with OASA(RDA), ODCSINT, DA, and other HQDA staff agencies having an interest in the issue.

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

(d) Provide to ODCSINT, DA (DAMI-CIT) a copy of proposals. ODCSINT, DA (DAMI-CIT) will notify the OSD member of the NDPC as necessary.

(7) The releases are reported to the FORDTIS.

(8) Documentary CMI and CUI will be released under this program only after the test program has been approved by both parties.

3–7. Disclosure of CMI and CUI in Security Assistance-Related Training

Training of foreign representatives at DA facilities or at DOD contractor facilities under the auspices of DA is to be in accordance with AR 12–8 and AR 12–15. (See para 5–13 for information regarding the conduct of orientation tours and visits; and see AR 12–15 for information regarding the exchange of small units for training.)

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

(1) Training involving access to CMI or CUI pertaining to tactics, techniques, and tactical doctrine for the training and employment of military forces (Category 1 information) will be within the scope of international RSI (AR 34–1) agreements. These agreements will be approved in accordance with paragraph 2–7, and the governments of all trainees will be parties to such agreements.

(2) Training involving access to CMI or CUI incorporating technical data pertaining to the operation and maintenance of specific US equipment items or weapons systems (Category 2 information) will be permitted only after the prospective trainee's government has signed a purchase agreement.

(3) Training involving access to CMI or CUI pertaining to applied R&D matters (Category 3 information) will be limited. Any CMI or CUI contained must be within the substantive scope of international cooperative R&D agreements and approved in the manner prescribed in Section III, below.

(4) Training will not involve access to classified production information (Category 4).

(5) Training involving access to information in Categories 5 through 8 will be carefully considered in light of politico-military considerations, U.S. mutual defense commitments, and the inherent sensitivity of intelligence information.

b. When representatives of more than one foreign government are concurrently enrolled in the same course of instruction, and the course material contains CMI, the specific CMI will be equally suitable for disclosure to all participants.

c. Foreign representatives participating in training and training-related activities under AR 12-8 and AR 12-15 will do so on the basis of invitational travel orders (ITO) and not under the foreign visit request procedures outlined in this regulation. The ITO will be published by competent authority in accordance with AR 12-15, chapter 7. Authorities preparing ITO must have appropriate foreign government certificates of security clearance for trainees and foreign government assurances regarding the protection of the CMI and CUI provided to trainees. Receipt of these materials is to be reflected in the ITO and is an essential factor in authorizing DA agencies and commands conducting training to release DA CMI and CUI to foreign trainees. (See paragraph 1–1e(7) for guidance regarding access to NATO information.)

d. At the discretion of DA agencies and commands conducting or supervising training, course-related classified documentary material (such as, DA and school publications, student notes) may be authorized for retention by trainees. Such materials must be transmitted to the trainees via US security assistance officials located in the trainees' home country (see para 4–9).

e. A foreign national may conduct training on U.S. equipment that is classified or involves classified information if the item has been sold or otherwise provided to the foreign national's government and the U.S. Government has specifically approved the provisions of such training to any involved third party. This authorization to conduct training does not waive conditions and limitations, if any, which have been established under an ENDP for such item provided to the foreign government; such conditions and limitations will be strictly enforced.

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

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

3–8. Concept

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

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

(1) NATO or ABCA RSI (AR 34–1).

(2) International Cooperative R&D (AR 70–41).

(3) The Technical Cooperation Program (TTCP) (AR 70–23).

(4) MWDDEP and DDEP (AR 70–33).

(5) U.S.-Canada Defense Development Sharing Program (AR 70-66).

(6) Specific agreements covering one or more designated subjects (such as, multinational participation in Army proponent programs covered by BMDO).

c. Excluded are agreements that are principally administrative, for example, the International Professional (Scientist and Engineer) Exchange Program (AR 70–58) and the Personnel Exchange Program (AR 614–10).

3–9. Preparation and implementation of International Cooperative R&D Agreements

a. International cooperative R&D efforts involving the disclosure of CMI or CUI must be reflected in formal international agreements prepared under AR 70–41 and AR 550–51. Such agreements must be coordinated and approved in the manner prescribed in paragraph 2–7 for disclosure programs. DA personnel engaged in the preparation and implementation of international cooperative R&D agreements must understand that such agreements are considered to be "agreements in principle" only. Thus, the existence of an agreement neither obligates approval nor constitutes advance approval of the disclosure of any specific CMI or CUI. Such an agreement forms the basis for disclosure consideration.

b. An agreement must designate specific DA officials and organizations that may accomplish the exchange of CMI and CUI approved for disclosure under the agreement's auspices. These designees will be responsible for insuring that a reasonable quid pro quo is maintained. They must concur in any proposed disclosure within the scope of the agreement for which they are responsible. To facilitate prompt coordination, international cooperative R&D agreements must be approved by OASA(RDA) (SARD–IN) who will advise what further (or prior) coordination is required.

c. Each international cooperative R&D agreement or separate substantive annex is to contain mutually agreed upon parameters for information exchange. Additionally, each agreement is to be supported by a TA/CP (appropriately marked to preclude access by foreign representatives) providing an assessment of the technologies involved and precise disclosure guidance. Such guidance is to be approved by OASA(RDA). It will designate specific topics to be incorporated in the agreement. A DDL will accompany the TA/CP providing precise disclosure guidance and release authority for CMI and CUI and will be approved by ODCSINT, DA (DAMI–CIT).

d. CMI and CUI considered for disclosure within the scope of international cooperative R&D agreements is usually limited to Category 3 information. Also, requests for information (RFIs) and requests for proposal (RFPs) may require enclosure of supporting Category 8 threat or countermeasures information, which will enable foreign contractors to conceptualize the battlefield envisioned or employment of the specified weapon or system. It is essential to understand that CMI or CUI pertaining to materiel items that have completed operational suitability testing, have been approved for production, or are in production is defined as Category 2 information and is not to be approved for disclosure under the auspices of international cooperative R&D agreements. CMI or CUI to be considered for such disclosure is limited to that defined in AR 70–1 as "research (6.1)," "exploratory development (6.2)," and "non-system advanced development (6.3A)." Other types of R&D-related CMI and CUI are considered to be materiel item-system-specific and may only be considered for potential disclosure under the auspices of international cooperative R&D agreements. This will be accomplished only after a preliminary decision by the Army Acquisition Executive or OASA(RDA) authorizing foreign participation in the development of a specific system.

3–10. CMI and CUI disclosure regarding materiel changes and improvements

Approval must be obtained to disclose CMI or CUI involving hardware or software changes or improvements pertaining to a materiel item or system that is in or beyond full-scale development. These changes or improvements which, if incorporated, would significantly improve performance, decrease vulnerability to countermeasures, or otherwise constitute a modification work order (MWO), engineering change proposal (ECP), or product improvement proposal (PIP), must be approved by HQDA for disclosure. Proposals are to be referred to HQDA essentially in the manner prescribed in paragraph 2–7. A separate exception to NDP–1 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 exception to NDP–1.

3–11. CMI and CUI disclosure to foreign personnel integrated into the DA R&D structure

DA policies and procedures governing the integration of foreign personnel into the DA work force are contained in chapter 5, section IV. Such integration is often the result of and accomplished under the auspices of an international cooperative R&D agreement. Personnel would be assigned to perform duties related to various aspects of DA materiel RD&A activities. Foreign integrated personnel may not be assigned to duties that will require access to DA CMI or CUI beyond that within the substantive scope of the international cooperative R&D agreement and as specified in the DDL. Also, disclosure must be consistent with the policies prescribed in this regulation. It is essential to recognize that—

a. Exceptions to NDP–1 will not be submitted for consideration by HQDA solely to provide for or facilitate such integration.

b. Such integration may not constitute any form of training, as defined in security assistance-related policies (AR 12–15).

c. Such integration is not to be used to circumvent certain materiel-related disclosure restrictions prescribed in this regulation (such as, regarding foreign access to item-specific or system-specific R&D CMI or CUI prior to a determination by HQDA of willingness to sell or transfer).

3–12. Foreign participation in classified contracts

The requirement to consider foreign industrial participation in classified Army contracts will require early consideration of foreign disclosure issues. The procuring contracting officer (PCO) is responsible for obtaining an Army position on foreign participation. This position must determine which foreign nations may be eligible to receive the CMI or CUI involved in the contract. Successful foreign participation in cooperative developmental contracts, either as a prime or subcontractor, may necessitate release of sensitive data. Therefore, the Army program managers or item managers must involve their headquarters FDO prior to advertising in the Commerce Business Daily and consider such issues as:

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

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

c. The maximum eligibility level for classified material in each NDP–1 category that may be involved. It is essential to remember that 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. Category 4 CMI can only be released with an exception to NDP–1.

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

e. The advisability of requesting a DDL for the procurement actions. The DDL will designate the specific disclosure authority for the solicitation and contract if it is awarded to a foreign firm.

Chapter 4
Modes, Methods, and Channels for CMI and CUI Release and Related Administrative Procedures

Section I
Procedures for Release to or by Visitor, Exchange, and Liaison Personnel

4–1. Introduction

a. In no instance may DA CMI or CUI be released or transmitted to other than the authorized representatives of the foreign government(s) or international organization(s) for which disclosure has been approved in accordance with the policies and procedures prescribed herein.

b. Disclosure of DA CMI or CUI may occur in one or more of the following modes: oral, visual, documentary, or materiel.

c. Disclosure of DA CMI and CUI may sometimes be accomplished 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 US companies performing work under contract to DA. Visits include attendance at or participation in meetings, conferences, and symposia sponsored or cosponsored by DA elements.

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

(2) Integration of—

(a) Foreign representatives into the DA work force.

(b) DA representatives into the work forces of foreign governments and international organizations.

(3) Certification of—

(a) Foreign LNOs and standardization representatives to DA.

(b) DA LNOs to foreign governments and international organizations.

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

(5) Requests initiated by US agencies—other than DA—for DA-originated CMI and CUI.

d. FOIA requests from or on behalf of a foreign government or foreign national will be processed under AR 25–55.

e. Succeeding paragraphs address release of DA CMI and CUI. Discussion focuses on the various modes and methods identified in *b* and *c* above and DA participation in various international activities.

f. DA officials authorized to release CMI and CUI are designated in paragraph 2–11.

4–2. DA CMI and CUI released during visits

a. Visits identified in paragraph 4–1 are further subdivided and categorized as follows:

(1) Visits to DA elements and DA contractors by—

(a) Foreign representatives at the formal invitation and expense of DA or DOD.

(b) Canadian personnel pursuant to formal US-Canadian agreements providing for the cross-border movement of military forces, in accordance with AR 525–16.

(c) All other foreign representatives, irrespective of the source of the initiative or funding, in accordance with chapter 5 of this regulation.

(2) Visits by US personnel to establishments of foreign governments and international organizations, in accordance with AR 1–40.

b. Release of CMI or CUI in conjunction with a visit is contingent on approval of disclosure to the foreign government or international organization involved. Such disclosure determinations will be made by DA officials possessing appropriate disclosure authority at the lowest command or supervisory level. Following such approval—

(1) DA personnel traveling OCONUS under AR 1–40, if such travel involves official interaction with foreign representatives, may be authorized to release DA CMI and CUI. The fact that and extent to which such authorization has been granted—in terms of both substance and mode of release (such as, oral, visual, documentary, or materiel)—are to be reflected in area clearance-related communications prescribed in AR 1–40. Releases accomplished in this manner are subject to all administrative requirements prescribed in Section II. The provisions of AR 380–5, chapter 8, also apply when U.S. personnel in temporary duty (TDY) status hand-carry CMI in documentary form.

(2) DA personnel may be granted authorization to release DA CMI and CUI to visiting foreign representatives. However, release will not take place until appropriate DA officials receive satisfactory written evidence that certain conditions have been met. These conditions include verification that the visitors possess appropriate security clearance and a complete justification for the level of CMI or CUI. Finally, the visitors' parent foreign government or international organization must accept full responsibility for protecting the CMI or CUI to be released.

(a) For visits conducted under chapter 5, visitors' security clearance status and the required security assurance will be conveyed via official foreign requests for visit authorization (RVAs). RVAs are processed in the manner described in chapter 5.

(b) For other visits, the DA sponsor is responsible for obtaining and disseminating clearances as well as security assurances. These will be communicated to prospective DA hosts. Such data may be acquired from a CONUS-based foreign military attache office or the appropriate USDAO. In the case of personnel assigned to NATO, the applicable U.S. national military representative or US liaison office will be contacted.

c. CMI and CUI approved for disclosure and release in conjunction with visits must be limited to information that is essential for successful accomplishment of the purpose of the visit. What is considered essential will be viewed from a U.S. perspective only. US-sponsored visits are normally arranged by U.S. personnel, and suitability of CMI and CUI for disclosure will be determined prior to tendering the invitations to preclude communicating false impressions.

d. Release of CMI by DA visitors to foreign establishments may be made in any mode, subject to a determination that disclosure is mission essential. Disclosure to foreign visitors to DA and its contractors will normally be in an oral or visual mode, or both. At the discretion of the DA host or command, however, an exception allowing release in documentary form may be made, per international or specific bilateral or multilateral agreement providing the DA host or command has a DDL covering the information to be released.

(1) Visitors requesting CMI in documentary form will be given guidance if this release is not covered by authorized agreements or participation in joint R&D activities. Such visitors will be told that such requests must be submitted in writing to HQDA or the appropriate disclosure authority by the visitors' military attaches (or designee). The submission of the request must cite that the purpose of the documentary request is the direct result of a specific visit and will support interoperability in some specific manner (para 4–7).

(2) If visitors are permitted to take notes during briefings or discussions involving CMI, the DA host agency or command will transmit such notes in the manner prescribed for document releases in paragraph 4–7 and section II.

4–3. DA CMI and CUI released to or by exchange personnel

U.S. and foreign exchange personnel retain their national identities even while serving in an exchange capacity. They operate under the supervision of and perform duties assigned by the host government or international organization. Exchange personnel do not serve as official representatives of their parent governments. They do not serve as official conduits for the release or transmission of CMI and CUI between their parent and host governments or organizations. CMI or CUI disclosed to exchange personnel is disclosed only for their satisfactory performance of assigned duties.

a. Access to CMI and CUI will be restricted to information that has either already been released to the exchange individual's parent government or organization or for which approval is obtained to release to the parent government or organization. It is to be written within the substantive scope of an existing disclosure program. Exceptions to NDP–1 disclosure policies will not be considered solely to accommodate such exchange. The prevention of subsequent misunderstandings and the ability of integrated personnel to fully perform anticipated duties must be considered. It is imperative that for each exchange individual a highly detailed job description be prepared by the prospective DA host element. This description must be approved by applicable disclosure authorities prior to negotiating any agreement providing for exchange or suggesting assignment to a specific duty position. (See para 3–11 for further details concerning DA integration of foreign representatives.)

b. DA personnel integrated into the work force of a foreign government or international organization may be provided DA CMI and CUI consistent with their degree of security clearance and valid need-to-know. The need-to-know of DA integrated personnel rarely exceeds that DA CMI and CUI deemed suitable for disclosure to the host foreign government or international organization. This does not preclude release to DA integrated personnel of US CMI that is essential to preserving US interests regarding RSI (such as, US CMI necessary for operational integration of US and allied forces or weapons systems). Unless the physical security requirements of AR 380–5 are fully satisfied, DA integrated personnel will not possess DA CMI or CUI in documentary form if disclosure to the host foreign government or international organization has not been approved.

4–4. A CMI and CUI released to or by certified liaison officers

a. Foreign LNOs are official representatives of their parent governments and international organizations. They act exclusively on the authority of and within the framework of mutually acceptable "terms of certification". The terms of certification are derived from and are consistent with the scope of existing bilateral and multilateral international and functional agreements. Foreign LNOs are certified to individual DA MACOMs specifically to further the objectives of such agreements. The authority to approve or deny the disclosure of DA CMI and CUI within the framework of these agreements is largely delegated to HQDA staff agencies and

MACOMs (chap 2, sec II). ODCSINT, DA (DAMI–CIT) delegates additional disclosure authority, as necessary, via the DDL accompanying approved terms of certification.

b. Disclosure of DA CMI and CUI to foreign LNOs is limited to information that has been shared with or approved for sharing with their parent government or international organization contingent upon the information having a direct bearing upon their assigned duties as defined in their DDL. When a foreign government or international organization has specifically requested their LNO be recognized as an official government conduit and if authorized in a DDL, DA CMI and CUI adjudicated releasable to the foreign government or international organization may be provided to foreign LNOs as an expeditious government to government transfer. Approval is given by the HQDA staff agency or MACOM to which the LNO is certified. A request that is within the terms of certification but involves DA CMI or CUI that exceeds the disclosure authority delegated to the agency or MACOM receiving the request will be referred to ODCSINT (DAMI–CIT) in accordance with paragraph 3–2 *b*. Notwithstanding the disclosure criteria, any request for documentary release must be accomplished in writing. It is further subject to the administrative requirements prescribed in Section II of this chapter. A submitted request involving DA CMI or CUI beyond an LNOs substantive terms of certification will be returned to the LNO and an entry made in FORDTIS. The fact that the request is beyond the terms of certification is explanation enough for the denial.

c. DA LNOs certified to foreign governments and international organizations may be authorized to release DA CMI and CUI on behalf of the HQDA staff agencies and MACOMs they represent. Release may be in oral, visual, or documentary form, depending on approval. Transactions will comply with the administrative requirements prescribed in section II.

4–5. DTIC document requests from specified governments

The 11 July 90 MOU signed by the Departments of Army, Air Force, and Navy, the Defense Intelligence Agency (DIA), and the Defense Technical Information Center (DTIC) established standard procedures for DTIC AD-numbered document requests for unclassified, limited distribution documents by the Government of Australia, Canada, and the United Kingdom. On 4 November 1991, HQDA implemented additional policies and procedures for DTIC to send requests from these governments for both classified and unclassified limited distribution documents and copies of documents directly to controlling office's foreign disclosure authority.

a. The Australian, Canadian, and British military attaches will submit all requests for classified and unclassified limited distribution documents to DTIC using a DTIC Form 55.

b. Requests will be processed as follows—

(1) DTIC will send Australian, Canadian and UK requests for both classified and unclassified-limited distribution documents, and copies of documents directly to originator or controlling office's FDO.

(2) The FDO will coordinate the request with the originator/controlling office.

(3) Originator/controlling office will conduct further coordination as required.

(4) If release is approved, originator/controlling office will sanitize and forward document through FDO to requesting embassy, and complete and return section III, Form 55B, to DTIC.

(5) If denial is recommended, return document and DTIC Form 55B, with justification for denial, to DAMI–CIT for final release determination.

(6) Fulfill FORDTIS reporting requirements as outlined in paragraph 4–10. If FORDTIS is not available, complete and forward DD Form 1822 to the command's MACOM. Army staff and MACOMs will forward the DD Form 1822 to DAMI–CIT.

(7) Originator/controlling offices should promptly return completed form 55Bs to DTIC. A prompt response will reduce needless administrative workload and preclude 90 day DTIC reminder notices to originators and HQDA (DAMI–CIT).

c. Each command having cognizance over information involving proprietary data is hereby delegated authority to respond directly to requesting government, even when release of proprietary data is denied. Command will comply with the following procedures—

(1) Coordinate with contracting office to determine if proprietorship is still current and valid. If current, contact author for release determination.

(2) Inform appropriate embassy of denial with copy furnished to DAMI–CIT. Provide rationale for denial (for example, "This is an english translation of a Japanese magazine article protected by copyright laws" or "Author does not grant permission to release his information to a foreign government".)

(3) Enter denial in FORDTIS. If FORDTIS is not available, complete and forward DD Form 1822 to the command's MACOM.

(4) If request received from DTIC, complete and return section III, Form 55B to DTIC.

4–6. JCO-certified contractors

The U.S.-Canada Joint Certification Office (JCO) certifies US and Canadian contractors to be eligible to receive controlled unclassified technical data controlled by DOD for legitimate business purposes. Further information on the JCP can be found in the DOD Pamphlet, "U.S.-Canada Joint Certification Program," published by OUSD(P) and dated March 1991.

a. Requests for CUI.

(1) Certified Canadian contractors are authorized access, identical to U.S. contractors within the limits of the ITAR, to CUI controlled in accordance with AR 70–31 and available through libraries, technical data repositories (such as DTIC), and DA contracting offices in accordance with distribution statements placed on such data per AR 70–11.

(2) Certified Canadian contractors may request DA CUI needed to respond to solicitation announcements (for example, Requests for Proposals (RFPs)) directly from the controlling DA office.

b. Processing Requests for CUI.

(1) Requests for DA CUI by a Canadian contractor MUST be accompanied by the following:

(a) A current certification form, DD 2345, "Militarily Critical Technical Data Agreement," which has been approved by the US-Canada Joint Certification Office.

(b) A statement of intended use of the CUI that falls within the scope of the business activity, as stated in the DD Form 2345.

(2) The controlling DA office will—

(a) Determine whether proprietary or limited rights to data desired will be violated (such as, containing third party information). These requests will be denied unless written consent is obtained from the owner.

(b) If the information is determined to be releasable by the proponent, approve the request and inform DTIC to release the information to the requestor.

(c) If the request is denied, subject to national security considerations, provide written explanation of the reason for denial to the requestor. If the reason for denial cannot be given to the requestor, the proponent of the information will forward the reason for denial through foreign disclosure channels to ODCSINT, DA (DAMI–CIT). ODCSINT, DA (DAMI–CIT) will decide whether to release the reason for denial to the Canadian government.

4–7. Other Releases of DA CMI and CUI

Most disclosures of DA CMI and CUI occur through the direct personal interaction described in the preceding paragraphs of this section. However, certain types of foreign requests are not prompted by personal interaction. These types of requests are for release of DA CMI and CUI in documentary form. They are submitted to ODCSINT, DA, unless (as noted in para 1–20 *d*) ODCSINT, DA has specifically authorized other channels to be used. The subparagraphs below describe the channels and methods to be used for processing such requests.

a. Foreign requests for Category 2 CMI and CUI pertaining to equipment items and weapons systems will be submitted or referred

to AMC/USASAC. The submission will be through established security assistance channels. This procedure will also be used for requests for various DA publications and other documentary materials potentially eligible for acquisition from FMS publications accounts established under AR 12–8, chapter 13, or AR 310–2/DA Pam 310–25, chapter 3. On receipt, AMC/USASAC will—

(1) Coordinate with Office of the Deputy Chief of Staff for Intelligence, HQ AMC, to ensure that the request is within the substantive scope described above, that the request has been authenticated by a foreign representative authorized to submit security assistance-related requests, and that the foreign representative is authorized to receive the requested information.

(2) If the request is legitimate, coordinate with all interested DA parties and approve or deny the disclosure. This action will be pursuant to AR 12–8 and the policies prescribed in chapters 1 and 2 of this regulation.

(3) Respond on behalf of DA to the applicable CONUS-based foreign military attache (or designee) using applicable security assistance channels laid out in DOD 5105.38–M.

b. Approved international cooperative R&D agreements may designate specific channels for responding to requests. If so, requests must be submitted through those channels. On receipt of requests, DA authorities and establishments designated in an agreement are to—

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

(2) Accomplish necessary coordination among other interested parties within DA, as prescribed in paragraph 3–2.

(3) Approve or deny the disclosure or refer the matter to the HQDA staff agency or MACOM exercising disclosure authority.

(4) Respond on behalf of DA. The approved materials will be provided to the applicable CONUS-based foreign military attache (or designee), USDAO or U.S. security assistance office.

c. Under conditions of actual or imminent hostilities, any Unified or Specified Commander may disclose CMI through the level of TOP SECRET to an actively participating allied force when support of combined combat operations requires the information. The Chairman, Joint Chiefs of Staff (CJCS), will determine, as soon as practicable, the limitations that should be imposed on continuing disclosures of the information and inform the US commander and the Chairman, NDPC. The appropriate US commander will notify the CJCS of such disclosures.

d. Foreign requests for documentary information pertaining to matters other than in the preceding subparagraphs will be initiated by the embassies according to table 4–1 and the accompanying notes. When the table's instructions stipulate the request will be sent to ODCSINT, DA (DAMI–CIT), these requests, if validated, will be—

(1) Logged in and assigned a case number.

(2) Coordinated with external organizations as required.

(3) Staffed to the controlling HQDA staff agency or MACOM having cognizance over the information.

(4) The recipient, if the proponent, is to obtain a copy of the document, review and complete Army coordination as needed for release. In all correspondence, both the DAMI-CIT case designator and any embassy reference should be cited. On receipt, the action agency or MACOM is to coordinate with all DA agencies or commands having an interest in the document's contents.

(5) If release is approved—

(a) Mark the document according to paragraph 4–8 *d* and *f*, below, and forward to the requesting embassy.

(b) Provide DAMI–CIT a copy of the letter to the embassy.

(c) Fulfill FORDTIS requirements IAW paragraph 4–10, below.

(6) If denial is recommended for other than proprietary reasons, forward a copy of the document with justification for final release determination to DAMI–CIT. For proprietary denial, notify the embassy and provide DAMI–CIT a copy of the letter.

(7) The recipient, if not the proponent, will refer such requests to the HQDA staff agency or MACOM that exercises proponency disclosure authority along with any comments or recommendations by the original action agency or MACOM plus all interested DA parties with which coordination has been accomplished.

Section II
Administration

4–8. Concept

Before DA CMI or CUI approved for foreign disclosure is released in documentary form and to avoid false impressions and proliferation of requests for CMI that clearly are not releasable to the requestor, certain actions are required. The DA agency or command approving disclosure will do the following prior to release of the material:

a. Delete references to non-releasable documents as well as non-releasable information. Responsibility for deleting unreleasable information from a technical document lies with the proponent or, in the case of a cooperative agreement, the technical coordinator for the Memorandum of Agreement (MOA). The proponent or technical coordinator will certify to the security officer that the publication has been sanitized to the extent necessary or that all references should remain in the proposed document less distribution lists. The release of DA pamphlets in the 310 series to foreign governments or international organizations eligible for security assistance is routinely approved if the pamphlets establish foreign military sales (FMS) programs.

b. Discourage disclosure of documents that are reference lists or are bibliographic in nature. To react favorably to justified foreign requests for information, identify the requestor's specific requirements and provide only the information that satisfies that requirement.

c. Discourage disclosure of documentary information in draft form. Normally, only the proponent exercising appropriate delegated disclosure authority will make such a disclosure determination. Examples of documentary materials are listed below.

(1) Classified solicitations.

(2) Operational test reports.

(3) Conceptual studies.

(4) Technical reports.

(5) Materiel test and evaluation reports.

(6) DA administrative, doctrinal, technical, and training publications.

d. CUI that contains foreign government information or proprietary information may NOT be released without approval in writing from the foreign government or contractor in question. The DA controlling office will ensure that all CUI information is properly marked with export warning and distribution statements in accordance with DODD 5230.24 (AR 70–11, app A) before release.

e. Remove or obliterate all distribution lists.

f. Select the applicable "Conditions of Release"statement(s) (see app E) and stamp, type, or legibly handwrite the statement(s) on the cover, title page, or first page of the documentary material.

g. "Bind" all documents through the use of staples or other fasteners.

h. Refer to paragraph 2–6 for policy guidance.

4–9. Physically conveying documentary material

a. CUI in documentary form may be physically conveyed to recipient foreign governments either by hand or by mail. If conveyed by mail, the material is to be addressed to the appropriate CONUS-based foreign military attache or USDAO. Release of CUI to foreign governments by OCONUS MACOM components of unified commands is to be accomplished in channels prescribed by the latter.

b. CMI in documentary form is to be conveyed in the same channels as prescribed for CUI in subparagraph *a*. In addition—

(1) CMI conveyed by mail is to be packaged and handled as prescribed in AR 380–5, paragraphs 8–102 through 8–104.

(2) For all CMI, whether conveyed by hand or mail, the releasing DA agency or command will use DA Form 3964 (Classified Document Accountability Record) to record the dispatch of the CMI and

obtain acknowledgement of its receipt. Receipts are to be retained as prescribed in AR 25–400–2 and AR 380–5.

c. CMI and CUI to be conveyed in documentary form to NATO agencies or commands are to be introduced into NATO channels in the following manner:

(1) If the information is conveyed by hand, the releasing DA agency or command is to ensure that the equivalent NATO security classification is properly affixed to the material, in accordance with AR 380–15 (see also AR 380–5, app A).

(2) If the information is conveyed by mail, the material is to be transmitted via the applicable US National Military Representative (USNMR) or U.S. Documents Office (USDOCO) identified in AR 340–25. CUI may be transmitted by ordinary mail, CMI must be transmitted according to AR 380–5, chapter 8.

(a) Letters of transmittal will contain the following statement: "The attached document(s) is(are) authorized for release into NATO channels; the (DA agency or MACOM) certifies that applicable NATO security markings have been affixed before the document was released into NATO channels."

(b) When DA MACOMs or agencies write classified documents intended for release to NATO, the following statement will be affixed to front and back cover sheets: "(US classification), releasable to NATO as NATO (classification)."

(c) Except as required by AR 380–5, chapter 8, receipts need not be obtained from USNMR or USDOCO addressees.

d. CMI and CUI to be conveyed in documentary form to multinational partners in cooperative projects that is not appropriate to all members of an international organization (such as, NATO) will comply with the procedures of this paragraph but be annotated on front and back covers: "(US classification), releasable to (list applicable countries) ONLY."

4–10. Recording CMI and CUI disclosure determinations and releases

a. All approvals or denials for foreign disclosure of CMI and denials of CUI will be recorded in FORDTIS. In the case of denials, DA disclosure officials must take special care to record a concise summary of the analysis that led to the denial. Denials for foreign disclosure of CUI are also to be recorded in FORDTIS.

b. FORDTIS is designed to record disclosure determinations involving CMI in seven types of cases. These cases are munitions licenses, export licenses, strategic trade issues, exceptions to NDP–1, visits by foreign representatives, certification of foreign representatives, and miscellaneous disclosure determinations (that is, all cases not related to the other six types). The DA agency or command that makes the disclosure determination is responsible for recording the data.

c. DA agencies or commands having FORDTIS terminals will record data on-line. Those not having an on-line capability will complete DD Form 1822 (Report of Disclosure/Denial of US CMI). DD Form 1822 will be forwarded through command foreign disclosure channels to the first level of command or technical supervision having an on-line capability. (Specific instructions governing both FORDTIS on-line entries and the completion of DD Form 1822 are contained in DOD 5230.18–M. DD Form 1822 is a controlled form which may be obtained through ODCSINT, DA (DAMI–CIT). ODCSINT, DA (DAMI–CIT) will provide copies to DA CMI and CUI disclosure authorities designated in paragraph 2–11. Copies may be made available to other DA agencies or commands on substantiated request to ODCSINT, DA (DAMI–CIT).

Table 4–1
Document Request Procedures

Item	If Information Desired is	and the Requester	and Information is	then the Requester Must
1	Available via the Government Printing Office (GPO) or the National Technical Information Service (NTIS). (See Note 1)	(N/A)	(N/A)	Aquire the information directly from the GPO or NTIS.
2	Contained in a Department of the Army administrative publication (e.g., Army regulation, pamphlet, circular, field/ technical manuel, ARTEP, etc.	a. Maintains a publications account with the USASAC. (See Note 2)	(1) UNCLASSIFIED	Acquire the information directly from USASAC.
			(2) CLASSIFIED	Submit written request to DAMI–CIT.
		b. Is not eligible to obtain a publications account with USASAC.	(N/A)	Submit written request to DAMI–CIT.
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 accredited to HQ, AMC	(1) UNCLASSIFIED	Acquire the information from USASAC. (See Note 4).
			(2) CLASSIFIED	Submit written request to DAMI–CIT.
		b. Is not accredited to AMC.	(N/A)	Submit written request to DAMI–CIT.
4	Contained in the US Army Service School publications (e.g., programs of instruction, lesson plans, special texts, study pamphlets, reference data and other instructional material).	(Same as Item 3)	(Same as Item 3)	(Same as Item 3)
5	In the form of training films or training aids.	(Same as Item 3)	(Same as Item 3)	(Same as Item 3)
6	Maps	(N/A)	(N/A)	Acquire the information from the Defense Intelligence Agency, ATTN: COS–4, Washington, DC 20301.
7	Contained in Military or Federal Standardization Documents (e.g., specifications, standards, handbooks and lists of qualified industries.	(N/A)	(N/A)	Acquire the information directly from the Standardization Document Order Desk, Bldg, 4D, 700 Robbins Ave., Philadelphia, PA 19111-5094.

Table 4–1
Document Request Procedures—Continued

Item	If Information Desired is	and the Requester	and Information is	then the Requester Must
8	Contained in professional magazines and journals (e.g., Army Magazine, Infantry Magazine, Armor Magazine, etc.)	(N/A)	(N/A)	Acquire the information directly from the publisher.
9	Under auspices of a legally approved Data Exchange Agreement or Information Exchange Agreement	(N/A)	(N/A)	May acquire the information only via Technical Project Officer to Techncial Project Officer.
10	Other than in items 1–9 above. (See Note 5)	Is certified to the Department of the Army	(N/A)	Submit written request to DAMI–CIT.

Notes:

1. Addresses for GPO and NTIS are:
   Superintendent of Documents
   Government Printing Office
   710 North Capital Street, NW
   Washington, DC 20402

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

2. Countries which are eligible to enter into Foreign Military Sales (FMS) arrangements with the US Army are *potentially* eligible to establish an FMS publications account with the Adjutant General's Office (TAGO) in order to obtain Army administrative publications. Military Attaches representing potentially eligible countries should inquire concerning eligibility status. For those eligible, the Army *expects* that such accounts will be established and maintained. The Director of Foreign Liaison will *not* provide administrative publications accounts with TAGO.
3. Other types of communications which are related directly to the actual or proposed acquistion of US Army equipment and material, under the auspices of Foreign Military Sales (FMS), also may be referred directly to the Commander, US Army Security Assistance Command, ATTN: DRSAC–SC, 5001 Eisenhower Avenue, Alexandria, VA 22333.
4. Requests for documentary information which are to be submitted directly to the US Army Security Assistance Command (USASAC) are to be prepared in accordance with the format and instructions depicted in Policies and Procedures Manual provided to all embassies by HQDA.
5. If a DDL authorizes a Liaison Officer (LNO) to request and receipt for documents relating to his certification, all embassy requests for these documents will be processed from the embassy through the LNO and not from the embassy to DAMI–CIT.

Chapter 5
Contact with Foreign Representatives

Section I
General Policy

5–1. Encounters with foreign representatives

All visits and assignments of foreign representatives to DA elements will be conducted under the International Visits Program or the Personnel Exchange Program and in accordance with this regulation.

5–2. Military attaches

Certain foreign personnel upon diplomatic accreditation by DOS and notice to DA by their respective foreign embassies are officially recognized by the HQDA Director of Foreign Liaison (DAMI-FL). This recognition is acknowledged in writing. Such a person is then a military (Army) attache for accomplishing official business with DA on behalf of his or her government. In recognizing a military attache, DA acknowledges that the attache has diplomatic status and is authorized by his or her government to act officially on its behalf in military matters. This recognition does not authorize the military attache to officially interact with DA elements or personnel other than the Directorate of Foreign Liaison, ODCSINT. It should not be confused with certification in a liaison capacity (described in para 5-26).

5–3. Disclosure of information

Disclosure of any DA CMI or CUI to any foreign representative will be in compliance with chapters 1 through 5.

5–4. Delegation of Disclosure Letter

A Delegation of Disclosure Authority Letter (DDL) will be prepared by the host DA activity FDO and contact officer, forwarded through foreign disclosure channels to ODCSINT, DA (DAMI-CIT) for approval, for each foreign national assigned to a DA activity as a liaison officer or under an exchange agreement (app D). While the DDL is intended for internal Army use only and will not be given to foreign representatives, the job description should be extracted and provided to the concerned foreign national.

5–5. Standards of appearance

All foreign visitors, including exchange, liaison and one-time visit personnel, if belonging to a military service, are expected to wear their countries' uniforms. Only when local U.S. military personnel are permitted to wear appropriate civilian attire should the foreign representative be permitted to wear civilian clothing. If foreign civilian personnel are visiting Army installations and offices, or local custom is for military employees to wear civilian clothing, a clearly identifiable badge should be given to the foreign representative to wear.

5–6. Contact officer

Contact officers will be designated to control activities of any foreign visitors, liaison officers, and exchange personnel at DA elements. While contact officers for one-time and recurring foreign visits (see para 5–16) may be designated verbally, they must be physically accessible to the foreign personnel during the entire visit. For liaison and exchange personnel, both a primary and an alternate contact officer must be in writing in paragraph 8 in the DDL. They must be physically accessible to and have daily contact with the liaison or exchange individual. All contact officers must be familiar with this regulation, other applicable guidelines governming the release of CMI and CUI, and specific disclosure guidelines established in the DDL. The local FDO will brief the contact officer of his duties. Contact officers also will adhere to the guidelines listed below. As a minimum, each contact officer is to perform the duties and functions outlined in this paragraph, which may be supplemented as necessary to meet local requirements.

a. Visiting foreign representatives. Contact officers for foreign visitors will—

(1) Become familiar with chapters 1 through 4 of this regulation, local supplementation, if any, and reportable foreign visitor activity under provisions of AR 381–12.

(2) Be briefed by the FDO and become familiar with the specific scope and classification of the approved visit.

(3) Coordinate with and obtain guidance from the following agency or command personnel:

(a) Foreign disclosure officer (concerning the preparation of briefings or discussion items requested by the visitors).

(b) Security manager or OPSEC officer (concerning agency or command activities occurring simultaneously with the foreign visit and from which visitors should be excluded).

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

(4) Prepare to receive and respond to confirmation of the visit and a possible request for administrative assistance by visitors or their military attaches.

(5) On request, assist in arranging for quarters or transportation; however, it must be made clear to visitors or their military attaches that all expenses involving quarters, transportation, and subsistence must be borne by the visitors. Because visits are occasionally canceled with little or no notice, contact officers should refrain from making commercial reservations for services on behalf of foreign visitors; rather, assistance should be limited to recommending and providing telephone numbers for commercial services.

(6) At the direction of the installation or activity commander, ensure that foreign visitors are aware of and comply with foreign disclosure and information security requirements pertaining to the visit. To that end the contact officer will coordinate with the FDO and will ensure that—

(a) Briefings and discussions do not exceed the scope and classification or sensitivity level approved for the visit.

(b) Any notes taken during classified briefings or discussions are collected and processed in the manner prescribed in AR 380-5.

(c) Information in documentary form as follows:

1. If classified, is forwarded to the local FDO for a release determination and then forwarded to the visitor's embassy or with proper authority released directly to the visitor. All requests for releases will be coordinated with the FDO.

2. If unclassified, is restricted to one copy each of documents directly related to the purpose of the visit (such as, text and supporting graphics of a briefing rendered to the visitor). Unclassified Army administrative, doctrinal, and technical publications are not to be provided as these are readily available for purchase by foreign governments through security assistance channels.

(d) Personnel with whom the visitors will have official contact or exchange information are made fully aware of information disclosure guidance and restrictions applicable to the visit.

(e) Access by foreign national visitors is limited to areas and information specified in each visit approval. Escorts are required when the visitors cannot otherwise be denied access to information or operations outside the scope of the approved visit.

(7) Notify ODCSINT, DA (DAMI-CIT) through foreign disclosure channels, when the designated contact officer is changed.

(8) Notify the supporting CI office of any foreign visitor activity which is reportable under the provisions of AR 381-12.

b. Certified liaison officer. The contact officer for a certified liaison officer (LNO) will—

(1) Be briefed by the FDO and become familiar with this regulation, the specific terms of certification approved by ODCSINT, DA (DAMI–CIT) for the individual LNO, and reportable foreign visitor activity under provisions of AR 381-12.

(2) Initially brief a newly certified LNO concerning DA and local policies and procedures affecting the LNO's status and performance of functions, as well as customs of the U.S. Army; subsequently, the contact officer will render advice and assistance to the LNO in complying with such policies and procedures. The contact officer will have the LNO sign a statement similar to one found in appendix F indicating his agreement and understanding.

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

(4) Receive, evaluate, and refer to the FDO for response, all the LNO's requests for information and coordinate responses with agency or MACOM foreign disclosure authorities, as necessary.

(5) Notify the ODCSINT, DA (DAMI–CIT) through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of foreign liaison officer under their oversight.

(6) Notify the supporting CI office of any foreign visitor activity which is reportable under the provisions of AR 381–12.

c. Exchange personnel. The contact officer for exchange personnel assigned to a DA element under a DA-sponsored exchange program will—

(1) Be briefed by the FDO and become familiar with this regulation, reportable foreign visitor activity under provisions of AR 381–12, and the exchange officer's approved job description, and contents of the approved DDL.

(2) Initially brief a newly assigned exchange officer concerning DA and local policies and procedures.

(3) Evaluate with the FDO proposals for consultations and visits outside the immediate organization to which the exchange officer is assigned, to ensure that such activities are essential to the successful performance of duties prescribed in the approved terms of certification; if so, arrange for such consultations and visits.

(4) Ensure that access to information is restricted to information approved for disclosure in conjunction with the exchange terms of certification and ensure that no information in documentary form is provided for retention by the exchange officer.

(5) Notify ODCSINT, DA (DAMI–CIT) through foreign disclosure channels when the designated contact officer is changed or upon permanent departure of the exchange person under their oversight.

(6) Notify the supporting CI office of any foreign visitor activity which is reportable under the provisions of AR 381–12.

5–7. Access to DA facilities

Foreign nationals may not have uncontrolled access to DA facilities. Representatives of allied and friendly countries, may be authorized unescorted access to DA facilities when all the following conditions listed below are met.

a. The foreign government concerned extends commensurate reciprocal privileges to U.S. in-country Army personnel.

b. Foreign nationals are sponsored by their governments, the need for frequent access is justified, and the required security assurance is provided.

c. Security measures are in place to control access to information and sensitive areas within the facility.

d. Access is required for official purposes on a frequent basis (that is, more than once per week).

e. A badge or pass is issued that identifies the bearer as a foreign national and is valid for a specific facility during normal duty hours.

f. The badge or pass is displayed on the outer clothing so that it is clearly visible.

g. The request for issuance of the badge or pass must be in writing and describe how provisions *a* through *f* will be met.

Section II
DA International Visits Program

5–8. 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, that the requesting foreign government provides a security assurance on the visitors, and to facilitate administrative arrangements for the visit.

5–9. Foreign Visits System (FVS) requirements

FVS, a sub-system of FORDTIS, was developed to enhance security and provide consistent application of policy in dealings with other

governments. By providing end-to-end automation support to the visits process, FVS improves responsiveness and the use of personnel resources by using state-of-the-art automation and communications capabilities, and by eliminating the need to handle over two million pages of paper each year. Most embassies in Washington, DC have joined the FVS users group. Using software provided by DOD, embassy personnel create visit requests which are transmitted via a dial-up connection to the FVS communications processor. The requests are then sent to the FVS central processor which distributes them to one of four Defense Visit Offices (DVO) located in Army, Navy, Air Force, and the Defense Intelligence Agency. The DVO's provide a staffing scheme which is returned to the central processor for dispatch of request information to the staffed facilities either electronically (*on-line* facsimile or message) or by written memo. Upon receipt of staffing responses, the DVO renders a decision which is returned to the embassy over the same path used for submission. At any time, both embassy and DVO personnel have immediate access to visit request status information. Requests for visits submitted by foreign governments will be submitted and processed using the FVS in accordance with FORDTIS procedures. These procedures are disseminated to all foreign government embassies by the FORDTIS office. Requests must be submitted at least 30 days in advance (21 work days) of the proposed visit. Visit requests which do not meet the 30 day requirement must have sufficient justification and are subject to the acceptance or denial by HQDA (DAMI–CIT). Requests for visits by governments that do not participate in FVS will be submitted in writing to ODCSINT, DA (DAMI–CIT) for processing.

5–10. Requests from countries without a military attache

If a foreign government does not have a military attache diplomatically accredited to the United States, the senior U.S. military representative located in the prospective visitors' parent country may prepare and submit the RVA to ODCSINT, DA (DAMI–CIT) for consideration. The RVA must conform to the policies and procedures for submission of RVAs in this regulation and DODD 5230.20. (Contact with non-DA elements should cite DODD 5230.20 instead of this regulation.) The RVA should be submitted via electrical message.

5–11. Foreign-owned U.S. companies

Foreign-owned U.S. companies are not foreign companies. They are incorporated in the U.S. and are subject to U.S. laws and regulations, including the Arms Export Control Act (AECA) and Export Administration Act (EAA).

a. There are no restrictions on release to these companies of unclassified technical data controlled by the AECA or EAA, provided access within the company is limited to U.S. citizens and intending citizens (formerly immigrant aliens). Any U.S. company, foreign-owned or U.S.-owned, must obtain the appropriate license or other written U.S. Government approval before the technical data can be exported or provided to a foreign national employee or other foreign person.

b. Decisions on the release of classified technical data to foreign-owned U.S. companies are dependent on the type of information involved and type of facility security clearance under which the company is operating. The most frequently employed arrangements to mitigate or negate foreign control or influence are as follows:

(1) The voting trust is used to transfer legal control of a company to trustees who are U.S. citizens. While the foreign owner retains equity ownership rights, the company is insulated from the foreign control and influence. Foreign nationals cannot have access to CMI or supervise classified contracts. There are no restrictions on access to CMI provided the firm is cleared at the appropriate level and requires access to perform on a government contract.

(2) The proxy arrangement provides for the legal title to remain with the foreign interests but the company is nevertheless insulated from foreign control and influence. This arrangement, and access to CMI, is the same as the voting trust arrangement.

(3) The special security agreement (SSA) allows the foreign parent firm to exercise general management. However, the day-to-day management of the company must be done by U.S. citizens. Foreign nationals cannot have access to CMI or supervise classified contracts. When a contractor has been cleared under the SSA, the clearance is valid for use by all DoD components that may have a need to contract for classified work, subject to the provisions and limitations of each applicable agreement.

(4) A company may be eligible for a reciprocal facility security clearance when the foreign ownership, control or influence (FOCI) stems from a country with which the U.S. has concluded a government-to-government security agreement that provides for this type of arrangement. Because foreign ownership or control remains in place, and foreign nationals may be employed by the company, reciprocally cleared companies may only have access to CMI determined to be releasable to the government of the ultimate parent company. Of the four types listed here, it is only in the case of a reciprocally cleared firm that a *foreign disclosure* decision is required.

(a) A reciprocally cleared company may prepare and submit RVAs directly to DA organizations, agencies, installations, facilities, or contractors or nongovernmental associations under DA security cognizance. These visits are processed under visit procedures outlined in DoD 5220.22–M (Industrial Security Manual for Safeguarding Classified Material). Access limitations imposed on a reciprocally cleared contractor apply equally to all employees of such contractors. It is the responsibility of the visited agency to ensure that the access limitations of the reciprocal facility clearance are observed. Involvement of the foreign military attache is not required.

(b) A U.S. wholly-owned subsidiary can represent its parent foreign company when doing business with either an Army organization or contractors doing business with the Army under the following conditions:

1. Visit requests, whether unclassified or classified, will be passed from the U.S. firm's security manager to the security manager of the Army organization or defense contractor.

2. If classified information is involved, there must be a contractual arrangement between the U.S. subsidiary and the parent (foreign) firm *before* such representation can take place.

3. There must also be a license in place or U.S. government approval prior to the U.S. subsidiary sharing export controlled information or CMI with the parent company.

5–12. Out of channel visit requests

RVAs sent directly to DA agencies or commands by other U.S. Government departments or agencies—or nonmilitary international organizations in which the U.S. Government maintains membership (such as the United Nations)—will be immediately referred to ODCSINT, DA (DAMI–CIT).

5–13. U.S.-sponsored visits

Sponsored visits are invited visits to the United States by foreign dignitaries. Foreign dignitaries are invited as guests of the Secretary of the Army, Army Chief of Staff, major commanders, HQDA principal in the name of the Chief of Staff, Secretary of Defense, or Chairman of the Joint Chiefs of Staff. They may also be invited as part of security assistance or special programs. These visits involve the expenditure of appropriated funds.

a. HQDA DCSINT is assigned overall staff responsibility for all U.S.-sponsored visits by foreign nationals. The ODCSINT, DA, in coordination with other interested staff agencies—

(1) Plans and administers this DA program.

(2) Administers visits (including planning them when designated executive agent by DOD).

(3) Serves as POC, providing advice and guidance in the selection of Army installations to be visited when another military department is designated executive agent by DOD.

(4) Administers security assistance orientation tours (OTs) and school tours to Washington, DC, programmed by HQDA DCSLOG under AR 12–15, chapter 12.

(5) Directly coordinates with TRADOC and FORSCOM units for all tours or visits administered. TRADOC and FORSCOM will be information addressees on all messages tasking their activities.

b. HQDA DCSLOG is responsible for overall policy and guidance for school tours. HQDA DCSLOG is also responsible for conducting the annual selection committee meeting for OTs. (See AR 12–15.)

c. ODCSOPS, DA is responsible for overall policy and guidance for Latin America Cooperation Fund visits, which are conducted at the unclassified level. ODCSOPS, DA (DAMO–SSM) will, after coordination with ODCSINT, DA (DAMI–CIT), approve or deny the proposed visit concept by the U.S. Army Military Attache (ARMA) or Security Assistance Office (SAO) stationed in the Latin American country. Upon approval of the visit concept, U.S. ARMA or SAO—

(1) Makes direct coordination and submits a formal visit request to the CONUS-based U.S. Army activities to be visited.

(2) Visits the final approving authority for the MACOM or staff agency.

d. MACOMs and heads of HQDA staff agencies should—

(1) Refer all inquiries regarding visits and tours by foreign nationals to ODCSINT, DA (DAMI–FLT). When a proposed visit or tour is part of a separate program, coordination with ODCSINT, DA will occur when original staff action is initiated. Inquiries from news media representatives, foreign and domestic, concerning sponsored tours will be referred to the Office of the Chief of Public Affairs for response in coordination with ODCSINT, DA.

(2) Are responsible for planning iteneraries for visits or tours that fall within their responsibility; coordinating with MACOMs of the installations and activities to be visited; and administering the tours.

e. In planning tours or visits, the responsible commander or staff agency will take the following actions in coordination with other interested agencies:

(1) Prepare the overall fiscal year program of tours.

(2) Take the necessary budgetary action to provide funds to support the planned program.

(3) Establish the basic itineraries, including estimated dates of arrival in the U.S., areas of interest, places to be visited, and proposed visit dates at each installation or activity.

(4) Obtain concurrences from affected MACOMs and installations regarding the number, timing, and itineraries of tours and issue invitations and authorizations for the tours.

(5) Obtain required administrative data from appropriate U.S. representatives in the countries concerned.

f. In administering a tour, the responsible commander or agency will undertake the following actions in coordination with other interested agencies:

(1) Arrange tour directors and escort officers as required.

(2) Prepare detailed itineraries, arrange transportation and accommodations, and coordinate with affected MACOMs, installations, and activities.

(3) Prepare and disseminate required detailed information to concerned agencies, activities, and installations.

(4) As appropriate, arrange for official entertainment.

(5) Arrange for appropriate courtesies and assistance to visitors at ports of entry and exit; in Washington, DC; and at each installation and activity concerned.

(6) Arrange for photographic coverage of ceremonies and other events (such as arrivals, departures, presentations of mementos, luncheons).

5–14. Invitations and other prior coordination

Normally there are two ways visits to DA organizations, agencies, facilities, and installations by foreign representatives are initiated. One way is an invitation extended by DOD or DA personnel. The second way is by informal coordination by foreign representatives.

a. Invitations.

(1) In instances where it is desired to spend representational funds to invite foreign nationals or representatives to visit military facilities under Army sponsorship (for example, speakers, participants in research projects, and the like) and invitee will be provided an ITO or an honorarium, the following procedures will apply:

(a) Letter of invitation to the individual or organization extending an invitation to visit or participate in a specific activity will be prepared and forwarded under cover letter through command foreign disclosure channels to ODCSINT, DA (DAMI–FLC). The letter should include complete background information and any other details considered necessary to obtain approval for the proposed visit.

(b) DAMI–FLC will accomplish any necessary coordination with OASD(ISA) or other interested agencies prior to dispatch through the appropriate foreign attache. Upon notification from DAMI–FLC that visit has been approved, ITO or travel arrangements may be accomplished by the sponsor. An RVA from the foreign attache will not be required.

(2) Visits resulting from invitations involving the expenditure of security assistance funds (such as FMS, MAP, OR IMET) will do so in accordance with Army regulations governing such funding. Visitors will travel on ITOs published by competent authority. ITOs are to be used for foreign students training under security assistance programs.

(3) Other invitations extended to foreign representatives:

(a) DA agencies and commands extending invitations to foreign representatives must ensure:

1. The invitation includes a clear statement that the invitees or their government must defray all costs associated with the visit;

2. An RVA through the foreign governments's embassy is required; and

3. must be issued with sufficient time to allow for the submission of the RVA at least 30 days prior to the proposed visit date.

(b) Prior to inviting foreign representatives, DA agencies and commands must ensure current political-military factors are considered. Should any doubt exist, the agency or command will, through foreign disclosure channels, obtain concurrence from ODCSINT, DA (DAMI–CIT).

(4) Coordination will take place before one DA agency or command extends an invitation for visits to another DA element's installations, facilities, or activities. The DA agency or command desiring to extend the invitation will initiate coordination.

b. Other prior coordination. The fact that a visit begins by informal coordination does *not* preclude the need for an official visit request and authorization. This requirement must be clearly understood by all interested parties (prospective host and visitor, as well as the visitor's military attache) to avoid mutual confusion and embarrassment. Only accredited foreign military attache personnel may propose and request visits by their countries' representatives. These proposals and requests become official only on presentation of an RVA to ODCSINT, DA by attache personnel. Unofficial contacts with foreign counterparts often promote the success of potential visits. However, DA disclosure officials must remember that unofficial contacts are not binding on ODCSINT.

5–15. Functions in honor of or sponsored by foreign nationals

a. Army personnel may receive invitations to official functions in honor of or sponsored by foreign nationals in the Washington, DC area. Personnel receiving these invitations will inform the ODCSINT, DA (DAMI–FLC) on their attendance plans to ensure the Army is properly represented at these functions.

b. Outside the Washington, DC area, local commander should take measures to ensure the Army is properly represented at functions sponsored by, or in honor of, foreign nationals.

c. Military personnel should wear a uniform when appropriate. It should normally be worn when it is desirable for Army personnel to be readily identified and the function is—

(1) At the White House.

(2) In honor of a U.S. or foreign official.

(3) In honor of a national holiday (either U.S. of foreign).

(4) Attended by a substantial number of reserve component personnel.

(5) A formal social event for which the wearing of the uniform would be proper.

d. The standards for the type of dress normally stated in invitations are as follows:

(1) Casual—Civilian casual clothing.

(2) Civilian Informal—Business suit with tie.

(3) Duty Uniform—Army green uniform with black four-in-hand tie or uniform dictated by local policy.

(4) Uniform Informal—Army blue or white (seasonal) uniform with four-in-hand tie (male) or neck tab (female). Enlisted personnel may wear the class A Army green uniforms (female with skirt) with white shirt and black bow tie, four-in-hand tie before retreat) or neck tab (female) as a substitute.)

(5) Black Tie (semiformal)—Army blue or white dress uniforms with black bow tie; blue, white or black mess uniforms. Enlisted personnel may wear the Army green uniform (female with skirt) with white shirt and black bow tie (male) or neck tab (female).

(6) White Tie (formal)—Army blue and black evening mess uniforms.

5–16. Requests for visit authorizations (RVAs)

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 for a specified purpose.

b. Recurring visit authorizations. Recurring Visit Authorizations permit separate visits over a specified period of time, normally one year, in connection with a government-approved license, contract, or agreement or other program when the information to be released has been defined and approved for release in advance by the proponent of the information, local FDO, and appropriate DA disclosure authority. Authorizations will be valid for the duration of the program, subject to annual review and revalidation and any specific requirements of the U.S. Army.

c. Extended visit authorizations. Extended Visit Authorizations will be used to permit a single visit for an extended period of time, normally beyond 30 days. Extended Visit Authorizations will be used in the following situations:

(1) Foreign government contract or joint program (such as, joint venture or representative to a joint or multinational program.).

(2) Participation in an Army exchange program under the PEP or the SEEP.

(3) Training, except for those individuals on invitational travel orders.

(4) Certification as a liaison officer to a DA activity.

5–17. Assignment, evaluation, and processing of RVAs

a. Upon receipt in ODCSINT, DA (DAMI–CIT) an RVA is screened to determine compliance with basic DOD administrative requirements, and accepted or rejected for further processing.

(1) If rejected, it is returned with annotations reflecting the rationale for rejection.

(2) If accepted, it is assigned for action and information to appropriate Army addressees on the following basis:

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

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

(3) Referral of an RVA by ODCSINT, DA, is without prejudice; that is, referral indicates only that DA has administratively accepted the RVA for processing and is not to be construed as DA solicitation of concurrence, nor predisposition to approve the RVA.

b. In evaluating an RVA to an Army organization the following are administrative factors. If the response to any of the first three is negative, a recommendation should be made to ODCSINT, DA, to return the RVA to the requestor without action.

(1) Is the expressed purpose of the proposed visit understandable and sufficiently detailed to permit due consideration from a substantive perspective?

(2) Is the proposed visit date sufficiently in the future to permit necessary preparation for the visit and required coordination for disclosure determinations? Is the proposed visit date acceptable to the prospective host?

(3) Is sufficient justification for the visit and associated discussions included in the RVA to permit necessary information disclosure determinations?

(4) Is sufficient rationale presented in the RVA—or known to the action addressee or prospective host—to warrant intermittent, repetitive visits, if so requested?

c. In evaluating an RVA to an Army organization the following are substantive factors to 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, is classified. In either case, disclosure to foreign representatives requires substantiating the proposed recipient has a valid requirement for the information (need-to-know) and that such disclosure 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 accepting or declining the visit.

(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 any specific information—particularly CMI. Instead, each potential disclosure 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 a clearly defined DA international activity goal or objective?" If not, the RVA should be recommended for denial.

(3) If the response to the points above is affirmative, 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 points:

(a) What is the minimum classification level of the information that must be disclosed to accomplish each aspect of the purpose of the visit?

1. Unclassified information that has been previously approved for disclosure to the public under AR 70-31 and AR 360-5.

2. Unclassified information that is not suitable for disclosure to the public, but potentially suitable for official release to a foreign government?

3. Classified information at the CONFIDENTIAL or SECRET level?

4. Classified information that exceeds the authority of NDP-1?

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

(c) Given the category of information involved and the minimum classification level necessary for meaningful discussions, what type of coordination is necessary to obtain disclosure approval, and who may approve disclosures?

1. Any information approved for disclosure to the public may be disclosed to visiting foreign representatives at the discretion of the visited agency or command local FDO without external coordination.

2. Information that is UNCLASSIFIED but not in the public domain may be approved for disclosure to foreign representatives at the discretion of the visited agency or command local FDO, provided the information has been cleared for release by its proponen

3. Information that is classified CONFIDENTIAL or SECRET and is within the substantive scope of an existing international activity requires approval at the first level of command to technical supervision exercising disclosure authority delegated for that activity and category of information.

4. Information that is not within the substantive scope of an existing international activity requires approval by ODCSINT, DA. Such a proposal constitutes a new disclosure program and must be accompanied by complete justification. A proposal that would require an exception to NDP-1 will not be considered in conjunction with visits processed pursuant to this regulation.

d. Disclosure of information bearing a NATO classification may be authorized by any Army holder of such information, provided—

(1) The proposed recipient represents a NATO agency or command or a NATO member nation.

(2) A NATO security clearance certificate is presented as evidence that the recipient possesses the appropriate NATO clearance.

(3) The Army holder makes a positive determination of the proposed recipient's need-to-know the information in question.

e. Other disclosure related considerations include the following:

(1) If acquisition by a foreign government of an equipment item or weapons system that is fielded, in production, or type-classified would inherently necessitate access to related classified information—

(a) Only information in the public domain may be disclosed if an exception to NDP-1 is required and not granted. If an exception is granted, classified information pertaining to the equipment item or weapons system may be disclosed.

(b) Only unclassified information may be disclosed to that government's representatives in the absence of a positive determination of U.S. willingness to sell the item or system. This willingness to sell is normally implied by either the Army's decision to release planning data on a government-to-government basis through security assistance channels or the granting of an export license for the commercial sale of the item or equipment by a DOD contractor.

(c) Pending final approval of the sale or transfer of Category 2 munitions or materiel, disclosure of classified information should usually not exceed the CONFIDENTIAL level and is to be restricted to general performance characteristics and information necessary to evaluate logistic or maintenance requirements stemming from acquisition. Category 3 R&D data requested by foreign governments interested in co-development programs will be handled on a case-by-case basis. Army program managers must determine the lowest practical level at which RFP's can be advertised. To allow fair competition for contracts by foreign industrial concerns, the level of disclosure must be common for both potential U.S. and foreign prime contractor participation. However, program managers have the authority to decide to restrict prime contract participation to U.S. industry and allow foreign industries to participate as subcontractors with only limited access to CMI or totally restricted to U.S. industries only. Procedures for limiting competition contained in the Federal Acquisition Regulation must be followed in all cases. A recommendation for release of a classified proposal to foreign governments will be submitted by the program security officer through command foreign disclosure channels to the supporting foreign disclosure office exercising disclosure authority for approval prior to the proposed advertisement date in the Commerce Business Daily.

(2) Information is exchanged as a consequence of a data exchange annex (DEA) or information exchange program (IEP) only on a quid pro quo basis. Thus, a proposal in which a DEA or IEP is the basis for disclosure requires the concurrence of the designated Army project officer or technical project officer (TPO) for the DEA or IEP; moreover, the TPO or designated alternate TPO is to be present during all such information disclosures.

(3) International agreements relating to cooperative R&D efforts may be cited in support of disclosures related to equipment items and weapons systems that have progressed beyond the R&D stage—this is, are type-classified and in production—as long as NDP-1 supports the Army's release of Category 2 information at the proposed classification level to the country or foreign organization.

f. Criteria for evaluating an RVA to a contractor facility includes the following:

(1) The activities of U.S. commercial firms are legally subject to the Arms Export Control Act (AECA), as amended. The AECA is administered by the Department of State, which implements the AECA via the ITAR. Included in the AECA/ITAR is the U.S. Munitions List, which defines in detail military-related materiel and technical data subject to AECA/ITAR control. The AECA/ITAR requires that a commercial firm acquire a munitions license from DOS before engaging in discussions or other substantive contacts with foreign representatives regarding items enumerated on the U.S. Munitions List—irrespective of whether such contacts occur within or outside of the U.S. Only three basic exceptions to this licensing requirement are available:

(a) No license for any country is required for contacts or discussions involving information that has been determined to be suitable for release to the general public. It is the responsibility of the U.S. commercial firm to obtain such determination from the applicable U.S. Government department having cognizance over the information.

(b) Generally, no license for Canada is required for contacts involving unclassified information.

(c) No license for any country is required if an authorized DOD disclosure official determines that such contacts are essential to further a valid, specific DOD international activity and elects to exercise the authority to exempt the commercial firm from the licensing requirements of the AECA/ITAR. Such action is termed "sponsorship" of an exemption to the AECA/ITAR on behalf of the commercial firm.

(2) Because it is not always possible for foreign representatives to determine whether sponsorship is necessary, DOD has published instructions requiring that foreign personnel notify DOD of their desire to contact U.S. commercial firms pertaining to materiel or information on the U.S. Munitions List. Such notification is to be made in the form of an RVA. The receiving service determines whether DOD sponsorship of an exemption to the AECA/ITAR is in DOD's best interests.

(3) In light of the AECA/ITAR provisions, the initial determination to be made on an RVA to a commercial firm is whether there are grounds for sponsorship of an ITAR exemption, that is, whether the stated purpose of the visit is directly related to an actual or planned U.S. government program.

(a) If not, the RVA will be denied. The visit may take place if the commercial firm discusses only information in the public domain or has obtained a munitions license applicable to the visit.

(b) If so, the request will be approved.

g. On receiving the concurrence or nonconcurrence, ODCSINT, DA (DAMI-CIT) will—

(1) On behalf of HQDA, officially respond to the RVA (approve or deny it).

(2) Notify the action addressee and others directly affected of any ODCSINT disagreements. Notification will be sent if the disclosure of classified information is beyond the disclosure authority previously delegated to the action addressee.

h. If the RVA is approved, notification to the requesters—

(1) Contains the name and commercial duty telephone number of the U.S. Army contact officer. This information will allow the prospective visitor or the requesting military attache to coordinate administrative arrangements. The duties and functions of persons designated as U.S. Army contact officers for visits of foreign representatives are outlined in paragraph 5-5a.

(2) Specifies that the prospective visitor or the requesting military attache must initiate contact and resolve administrative arrangements with the prospective host. Arrangements must be made not later than 3 working days prior to the visit date. (A reasonable, earlier deadline for administrative coordination may be specified by the prospective host when the action addressee's response is submitted to ODCSINT.)

i. Improprieties by foreign representatives while visiting a location under DA administrative control will be handled in accordance with applicable legal and regulatory requirements and be reported promptly to ODCSINT, DA (DAMI-CIT). DAMI-CIT may consult with the appropriate embassy authorities.

5–18. Visits by Foreign National Employees of U.S. Defense Contractors

Visits by foreign national employees of U.S. contractors to DA elements or to DA contractor facilities on official business do not require a visit request through foreign government channels. Access to export controlled technical data by foreign national employees of U.S. contractors are authorized pursuant to an export license or by other written U.S. Government authorization obtained by the employing contractor. When these employees visit a DA contractor facility or a DA element, the employing facility will provide a copy of the export license or other written authorization to the appropriate FDO or security office, as applicable, at the facility to be visited.

5–19. Visits for Foreign Participation in U.S. Procurement-Related Meetings

Potential foreign attendance must be assumed when planning for meetings that may lead to contract opportunities for nations with which the United States has reciprocal procurement agreements. Foreign attendance at such meetings will be handled according to chapter 4 and AR 380-5. In addition, the following procedures also apply:

a. Disclosure decision. A Program Manager will determine the extent to which CMI or CUI may be involved throughout the life cycle of a program and coordinate with the FDO and Contracting Officer to assure compliance with the NDP, DOD, DFAR, and HQDA regulatory requirements before the announcement of a procurement action. Decisions on disclosures of CMI or CUI will be in compliance with this regulation. The extent of foreign attendance at meetings related to the procurement action will be contingent on the disclosure decision. If attendance by foreign nationals is permitted, any CMI to be disclosed must be at a level authorized for disclosure to all foreign nationals who are present.

b. Denials. ODCSINT, DA (DAMI-CIT) will be the final adjudicating authority on a specific appeal by a foreign government for attendance by its representatives at such meetings.

5–20. Visits by Representatives of the North Atlantic Treaty Organization (NATO)

a. NATO business. Members of NATO organizations or commands attending NATO conferences or meetings or to conduct NATO specific business at an Army installation or DoD contractor facility do not require an embassy initiated visit request. Visitors must be serving as representatives of their NATO organization for the purpose of engaging in specific NATO, not national business. Clearance certification should be provided directly from the parent NATO organization to the meeting host who will accomplish the necessary local coordination. (See DoD Directive 5100.55 for additional guidance.) Recurring visits related to NATO Production Group (NIAG) activities will be processed according to AR 380-15.

b. Non-NATO business. Visits by representatives of a NATO command or agency or the NATO international staff, as well as personnel of NATO member countries, desiring to visit Army installations or DoD contractor facilities to conduct business of a national nature or to attend conferences or meetings as a national representative are required to submit a visit request through embassy channels.

5–21. Visits by Representatives of the American, British, Canadian, and Australian (ABCA) Program

Periodically, Army installations are required to provide a setting for ABCA meetings and to provide ingress and egress to the location. No disclosure issues are involved in that all U.S. information discussed in such a forum must have previously undergone proper disclosure review and be appropriately marked and authorized for release to ABCA.

a. ABCA information. Members of ABCA wishing to visit Army installations to attend ABCA conferences or meetings, or to conduct ABCA specific business at that site, will not require an embassy initiated visit request. Persons visiting must be serving as representatives of their ABCA organization for the purpose of engaging in specific ABCA, not national business. Ingress and egress authority is to be coordinated directly between the office hosting the meeting or visit and the local foreign disclosure authority. Clearance certification will be provided directly from the parent ABCA organization to the meeting host who will then accomplish necessary coordination.

b. Non-ABCA information. Members of ABCA wishing to visit Army installations to conduct business of a national nature or to attend conferences and meetings as a national representative, will be required to submit a RVA through embassy channels.

5–22. Canadian Visits Under the U.S.-Canada Joint Certification Program (JCP)

Under the U.S.-Canada JCP, procedures have been established to facilitate certain types of directly arranged unclassified visits by Canadian government officials and Canadian contractors to DA elements and DA contractor facilities. All other visits by Canadian contractors not outlined in this subparagraph will be processed in accordance with paragraph 5-17, above.

a. Canadian government officials and contractors are authorized to make direct visit arrangements with DA elements for the purpose of—

(1) Responding to an invitation.

(2) Collecting or discussing unclassified solicitations.

(3) The furtherance of procurement activity related to unclassified solicitations (such as, pre-solicitation conferences).

b. Procedures for unclassified contractor-to-DA element visits include the following:

(1) The Canadian contractor will provide the form DD 2345, "Militarily Critical Technical Data Agreement," to the host activity. A separate DD Form 2345 will be submitted for each proposed visit. Prior coordination will be made directly with the security office at the concerned element to arrange the visit.

(2) The host agency head or installation commander retains final approval authority for a visit. A visit may not be approved, however, without adhering to procedures in this regulation.

5–23. Processing RVAs to attend meetings, conferences, and symposim

Attendance by foreign representatives at any meeting, conference, or symposium that is sponsored, cosponsored, or hosted by a DA element must be authorized in advance by ODCSINT, DA. This authorization ordinarily is conveyed in the form of an approved RVA processed under paragraph 5-17. In certain instances involving duly accredited foreign LNOs, the requirement for submission and approval of an RVA may be waived at the discretion of ODCSINT (see para 5-28c(1)). (See chap 6 for detailed policies and procedures.)

5–24. Delegation of authority to approve certain visits by foreign representatives

a. Under certain circumstances as described below, the interaction of foreign representatives with DA elements may be considered unofficial. These circumstances include interaction that is or may be a consequence of a contractual arrangement not involving a foreign government. In this case, the HQDA DCSINT, delegates authority to specified heads of HQDA agencies and MACOM commanders to approve visits by foreign representatives to organizations, agencies, activities, installations, and facilities under their jurisdiction. Such visits must be consistent with OPSEC practices (See AR 530-1.). They will involve the disclosure of information approved for public

release or within the disclosure purview of the visited element. The agency head or MACOM commander may further delegate this approval authority to organizations, agencies, activities, installations, and facilities commanders.

b. Authority is generally delegated to approve—

(1) Visits to participate in social activities (irrespective of agency or command sponsorship or involvement), activities open to the general public (such as Armed Forces Day open house), or official activities to which members of the public have been invited (such as a wreath-laying ceremony).

(2) Visits to obtain authorized routine or emergency medical treatment.

(3) Transient visits (such as brief stopovers on a flight).

(4) Visits necessary in the performance of an unclassified contract with the visited agency or command or with another DOD component or Federal agency.

(5) Visits by U.S. citizens representing foreign companies holding reciprocal facility clearances.

(6) Visits by foreign media representatives under the auspices of the Office of the Chief of Public Affairs, HQDA or Office of the Assistant Secretary of Defense (Public Affairs).

(7) Visits by foreign dignitaries sponsored by another Federal agency and organized by the Office of the Assistant Secretary of Defense (Public Affairs).

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

(9) Visits by Canadian and Mexican government officials to DA organizations, agencies, activities, installations, and facilities in proximity to the borders of the United States. However, these visits must be as a direct consequence of a mutual interest in preventing or resolving border-related incidents involving Army personnel. The goal is to maintain good community relations.

(10) Attendance at pre-bid briefings and bid opening ceremonies. However, an invitation must have been extended by the DA agency commander to foreign defense suppliers and foreign government representatives.

c. Authority is specifically delegated to—

(1) The Chief of Engineers and The Surgeon General/Cdr, USAMEDCOM, to approve visits to organizations, agencies, activities, installations, and facilities under their jurisdiction, provided these visits—

(a) Are officially sponsored by other Federal agencies.

(b) Or, pertain solely to unclassified activities having no direct military application (that is, goods or services enumerated under the U.S. Munitions List and governed by the Arms Export Control Act).

(c) Or, are accomplished pursuant to official interagency agreements or specific involvement in bilateral or multilateral agreements for which other Federal agencies are the proponents.

(d) Or, are accomplished fully according to statutory and regulatory requirements pertaining to the use of DA resources in training foreign personnel (see AR 12-15).

(e) Or, are short notice requests from appropriate agencies or medical staff members from friendly countries for short duration visits to medical treatment facilities (normally not to exceed five days). The purpose of these visits is normally limited to specific patient treatment and related issues. These requests are not designed to supplant formal RVA procedures.

(f) The Chief of Engineers (COE) is delegated approval authority for the foreign participation in the unclassified U.S. Army Corps of Engineer Contracts program.

(2) The HQDA Assistant Chief of Staff for Installation and Environmental Management (ACSIEM), to approve visits to Army organizations, agencies, activities, installations, and facilities, provided these visits are in connection with the Army's participation in international sports activities. The prior concurrence of the DA agency or MACOM exercising jurisdiction over the location must be obtained.

(3) The HQDA Chief of Public Affairs, to approve visits by foreign news media representatives to Army organizations, agencies, activities, installations, and facilities. The concurrence of the DA agency or MACOM exercising jurisdiction over the location will be obtained prior to such visits. Foreign news media representatives will not be permitted access to CMI, CUI, or classified areas or activities during such visits.

Section III
Liaison Officers

5–25. Concept

a. Liaison officers (LNOs) are certified to DA elements to perform specific functions on behalf of their governments. 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 bilateral or multilateral international agreements. Foreign LNOs are certified to an individual DA MACOM, specifically to further the objectives of such agreements. Multiple certification as LNO to more than one MACOM is not authorized. In previous regulations, the certification process was referred to as "accreditation." The term "accreditation" now is used only to refer to legal recognition by the Department of State of a foreign national's diplomatic status.

b. DA liaison officer certification does not bestow diplomatic or other special privileges.

c. Activities of liaison officers will be limited to the representational responsibilities of their governments described in the certification. They are expected to present the views of their parent governments with regard to issues of mutual interest, namely issues that may be raised by the DA agencies and commands to which they are certified.

d. Liaison officers may not perform duties reserved by law or regulation to officers or employees of the U.S. Government (for example, an LNO cannot provide services or labor to the U.S. Army).

e. Liaison officers will be required to reside in the continental U.S. (CONUS) at or within normal commuting distance of the organizational element to which certification is proposed. Exceptions to residence and commuting requirements may be requested by the requesting MACOM, but only on an exceptional basis.

f. Liaison officers may assume custody of releasable documentary information when authorized in writing by their government and consistent with the terms of certification.

g. When operational requirements dictate, strict reciprocity is not required for liaison officer assignments.

h. DA certification will not be used to assign foreign nationals to DA contractor facilities. DA contractors must obtain an export license for such assignments and comply with provisions of DOD 5220.22-M, chapter 10. If the approved export license does not specify disclosure guidance, the contractor will request guidance from the Program Manager. Guidance will be approved by ODCSINT, DA (DAMI-CIT) in the form of a DDL.

5–26. Establishment of LNO positions

a. DA commands and agencies desiring to have foreign LNOs certified to them must first formally obtain HQDA concurrence in principle. This concurrence in principle will be obtained prior to beginning discussions with foreign representatives or, if initiated by a foreign government, prior to making a firm commitment to the government. Such initiatives will be conveyed in writing through command foreign disclosure channels to ODCSINT, DA (DAMI-CIT) for HQDA and OSD coordination.

b. LNO proposals, whether U.S. or foreign initiated, must—

(1) Clearly demonstrate or anticipate a mutual need for information exchanges. The information must be of such volume and scope as to require the LNO's physical presence on virtually a daily basis. Presumably, any lesser degree of interaction could readily be accomplished via authorization for a recurring visit. The proposed position must clearly serve the requesting command's as well as DA's best interests.

(2) Directly relate to or further a current or pending DA-approved international agreement. Personnel deemed essential to the successful execution of a treaty or international agreement may apply for certification as a liaison officer. Certification, however, will be approved only if such treaties or agreements pertain to foreign participation in mutual defense, co-development programs, coproduction of materiel, or the training of foreign personnel. Training must be under DA auspices and must relate to operating or maintaining materiel acquired from DA through security assistance channels.

(3) Be substantively and administratively consistent with similar certifications granted to U.S. Army personnel assigned to the foreign country of the nominees. It must also be consistent with Federal, DOD, and DA information disclosure policies. In addition to the criteria noted above, the nature of information proposed for acquisition or exchange by the LNO will be considered. The agency or MACOM will consider the extent to which such information could be disclosed to the foreign government in question under DA policies.

c. The proposal will include a draft Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA), as appropriate, between the command and the foreign government which outlines relevant commitments and procedures. Formal international agreements are required in two instances: when the foreign representative is coming from a country which has no status of forces agreement (SOFA) which applies within the U.S., and/or when the command intends to obligate appropriated funds to support the foreign representative. In these instances, the command must obtain permission to negotiate and conclude a formal international agreement in accordance with AR 550-51. This involves agencies within DoD and the Department of State. If the proposed foreign liaison officer or personnel exchange officer comes from a country that has a SOFA which applies within the U.S. (e.g., the NATO SOFA), and the command will provide only de minimus support to a liaison officer, then less formal procedures are permitted. A MOA/MOU should discuss at a minimum the following items:

(1) Accurate reference to applicable international agreements (e.g., bilateral health care agreements) and to a current SOFA which covers the status of forces. Currently, there are very few SOFAs that apply to foreign forces serving within the U.S. Several SOFA's apply to U.S. forces serving within other countries.

(2) Unless covered in an applicable SOFA, a MOU/MOA must address such items as: parties, purpose, duties, legal status, customs, taxes, temporary travel, medical care, claims, exchange/commissary privileges, criminal jurisdiction, disciplinary procedures, removal criteria and procedures, dispute resolution, uniform requirements, security, agreement termination, and any other necessary provisions. The U.S. may commit to providing benefits or obligating funds only in accordance with applicable laws and regulations.

(3) If the other country is sponsoring a reciprocal (one-for-one) exchange of liaison or exchange personnel, then the parties may agree to provide like support and services.

(4) For liaison and exchange personnel coming from countries that have entered a SOFA that applies within the U.S., the MOU/MOA should cover only those provisions not already addressed in the SOFA (e.g., no need to discuss status, customs, claims, taxes, jurisdiction).

d. Finally, the requesting MACOM or agency FDO will submit a proposed DDL outlining the terms to be applied to the certification. Such terms must state the precise nature of information recommended for disclosure and the associated level of classification. Also considered will be specific restrictions or limitations to information disclosure. Additionally, the DDL will identify the U.S. Army contact officer responsible to ensure compliance with the approved terms of certification. The contact officer will be briefed by the FDO on his/her responsibilities and must have a thorough understanding of DA information security and disclosure policies and functional familiarity with the substantive terms of the LNO's certification (see para 5-4b for further details).

e. Upon receipt of the proposal, DA ODCSINT (DAMI-CIT) will staff the proposal with appropriate offices and agencies. Upon concurrence, the command or agency will be notified that they may begin negotiations with the foreign government to finalize the establishment of the position(s) and obtain the signature of the appropriate foreign representative.

f. Once signed, a copy of the MOU/MOA and final draft of the DDL will be forwarded to DA ODCSINT (DAMI-CIT) for final approval. DAMI-CIT will coordinate approval of MOA with appropriate agencies.

5–27. Processing requests for liaison officer certification

a. Once a MOU/MOA has been approved, liaison officers will be processed under an extended visit authorization submitted at least 90 days prior to the requested date of assignment. On receipt of an administratively acceptable request for LNO certification (extended visit request if embassy is on FVS or letter signed by Military Attache), ODCSINT, DA will refer the request for consideration through command foreign disclosure channels to the DA agency or MACOM to which certification is requested. Such referral is not and will not be construed as HQDA predisposition to approve the request.

b. In addition to an extended visit authorization, in order to obtain certification of a foreign government liaison officer, the military attache of the foreign government must provide written notification to ODCSINT, DA (DAMI-CIT) advising that—

(1) Subject individual is an officially sponsored representative of that government.

(2) Such official is authorized by the sponsoring government to conduct business with the Department of the Army for purposes that must be specific, citing related agreements, contracts, or other arrangements.

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

(4) The official may assume custody of documentary information on behalf of the government.

(5) The liaison officer's government will assume the responsibility for any and all U.S. CMI or CUI provided to such official.

(6) A description of the legal status of the proposed liaison officer (including any privileges and immunities to which the liaison officer is entitled) and sponsoring government responsibilities.

c. The receiving DA agency or MACOM will evaluate the request and submit to DA a recommendation to approve or disapprove the request.

d. Upon receipt of the agency's or MACOM's recommendations for disposition of the request for LNO certification, ODCSINT, DA will decide on the request and formally notify the requesting embassy.

e. Subsequent to formal certification, any proposal to broaden the scope of an LNO's certification is to be referred to ODCSINT, DA (DAMI-CIT) with full supporting rationale. Any proposal to extend the LNO's duration must be initiated by the requesting embassy personnel utilizing FVS or by letter if the embassy is not on FVS. Extension requests will state under "purpose of visit request" extension of current visit with that visit request's number. Notification of an LNO's permanent departure or any change in contact officer must also be forwarded to ODCSINT (DAMI–CIT) by the U.S. command.

f. Once initially granted, each liaison position will be reevaluated on each successive nomination, to ensure that the best interests of the host agency or MACOM and DA continue to be served.

5–28. Administering liaison officers

a. Services provided. As official representatives of foreign governments, LNOs may not receive administrative, operational, or logistical services that involve the expenditure of, or are supported by, U.S. appropriated funds, unless such services are specifically authorized pursuant to an approved international agreement or are purchased by the foreign government. Typical types of services involved are use of office space or equipment, clerical and other administrative support, housing, travel, exchange and commissary privileges, and access to medical facilities.

b. Disclosure of classified information. Terms of certification approved for each LNO establish the maximum substantive scopes and classification levels within which disclosures of classified information may be made. As is the case with all access to classified information, the proposed recipient must have a need to know the information in question. In no case may any disclosure to a foreign LNO exceed the classification level established in the original certification without express approval of ODCSINT, DA.

(1) Unless specifically authorized by their government and the approved terms of certification, access to classified information by foreign LNOs is permitted in oral and visual forms only. If authorized access to classified information, an LNO may be included in discussions involving classified information and may be shown classified information in documentary form, provided such documentary materials remain under U.S. control. When authorized by their government and the approved DDL to receive information in documentary form, the LNO may also make and retain classified notes as a consequence of such discussions or observations. However, unless the receipt of documentary materiel is authorized by the DDL, the LNO is not permitted to reproduce the materiel in question (See paragraph 4-9).

(2) All certified foreign LNOs may request release of classified information in documentary form directly from host agencies and commands, provided the information in question is within the terms of certification. LNOs, when authorized by their government and consistent with the terms of certification, may be designated as an official channel of their government for the purposes of receiving classified information (see para 5-25d).

c. Visits.

(1) A visit by an LNO may be approved at the agency or MACOM level if the proposed destination is within the organizational jurisdiction of DA and the purpose of the visit is within the scope of the officer's approved terms of certification. MACOM disclosure officials are required to coordinate such visits between MACOMs and do not require official authorization from ODCSINT, DA.

(2) All visits to destinations outside the terms of certification or DA jurisdiction (that is, destinations under the organizational jurisdiction of other services, OSD, OJCS)—including unified and specified commands—and other Federal departments and agencies) must be initiated on the LNO's behalf by their embassy.

(3) Travel-related funding for all LNO visits is the exclusive responsibility of the officer's parent government.

(4) Travel on U.S. military aircraft by LNOs is governed by the provisions of AR 95-1.

d. Library and publications support. At the discretion of the host agency's or command's contact officer and through coordination with the FDO, an LNO may be granted access to unclassified sections of agency command libraries. Additionally, each LNO may be provided a reference set of DA and agency and command publications necessary to the successful performance of the officer's liaison duties and consistent with the officer's approved terms of certification. Publication reference sets are to be on loan, and such sets must be returned or transferred to the officer's successor when the officer's certification ends.

e. Computer access. Foreign LNOs may not have unsupervised access to computer systems (standalone or networked) unless the information accessible by the computer is releasable to their government.

f. Misconduct. Foreign LNOs serve at the pleasure of DA and are expected to conform to the Army's customs and traditions and comply with all applicable statutory and regulatory requirements. If a foreign LNO violates the terms of certification; violates statutory, DA, or local regulatory requirements; or otherwise conducts personal or professional affairs in a manner that is unsatisfactory to the host agency or command; the officer is to be reported in writing via command channels to the Director of Foreign Liaison, ODCSINT, DA (DAMI-FL). The report is to cite full particulars and contain a recommendation for final disposition by HQDA, for example, to refer the matter to the LNO's military attache for appropriate administrative action, to temporarily suspend or permanently revoke privileges, to suspend certification for up to 30 days, or to revoke certification.

Section IV
Exchange Personnel

5–29. Concept

a. In accordance with applicable exchange program regulations, foreign military and civilian personnel may be integrated into the DA work force to perform either general or highly specialized duties. Such exchanges must be in furtherance of a formal bilateral or multilateral agreement between the U.S. Army and foreign military establishment or of an agreement between the U.S. Army and another U.S. Federal agency, which may elect to act on behalf of foreign representatives. Such agreements must be formally coordinated with HQDA under AR 70-41 and AR 550-51. Unilateral assignment of foreign officers to U.S. positions without a reciprocal exchange violates statutory prohibitions against the acceptance of voluntary services by an agency of the Federal government.

b. The Army participates in only two programs that routinely involve the exchange of personnel: the Personnel Exchange Program (PEP) (proponent: ODCSOPS, DA (DAMO-SSF), under AR 614-10) and the Scientists and Engineers Exchange Program (SEEP) (proponent: HQ AMC, under AR 70-58).

c. Another standing program in which the Army participates is the TTCP, which can involve exchange of foreign personnel (proponent: HQ AMC, under AR 70-23).

d. The role of ODCSINT, DA, in implementing formal agreements providing for the exchange of foreign personnel is two-fold:

(1) In its coordinating staff capacity, ODCSINT reviews proposed MOU establishing exchange positions, associated job descriptions, and approves a DDL for each position for consistency with DOD and DA information disclosure policies.

(2) In its foreign liaison capacity, ODCSINT receives and processes foreign embassy-initiated nominations of personnel to be assigned to exchange positions. DA authorities consummating agreements providing for the integration of foreign representatives into the DA work force are to provide an information copy of the MOU to ODCSINT, DA (DAMI-CIT), in addition to copies deposited in accordance with AR 550-51.

5–30. Restrictions on exchange personnel

a. Exchange programs will not be used as a mechanism for exchanging technical data or other controlled information between the governments or for training of foreign nationals or instead of, or in combination with, liaison officer certification. Information exchanges will be governed by appropriate agreements (such as cooperative research and development or data exchange agreements); training of foreign nationals will be in accordance with security assistance procedures.

b. Foreign exchange personnel function under the operational and administrative control of the DA agency and MACOMs to which assigned. Consequently, such personnel are prohibited from acting as official representatives of their parent governments.

c. Foreign exchange personnel may not act in the dual capacity as an exchange participant and representative of their government while assigned to a DA component. (For example, an exchange participant may not act as a liaison officer.)

d. Foreign exchange personnel may not serve as conduits between DA and their government for requests and transmission of CMI and CUI.

e. Foreign exchange personnel may 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 U.S. Government, or that would afford them access to information that is not authorized for release to their governments.

f. Exchange personnel may not be given security responsibilities. (For example, escort responsibility, document custodian, or security checks.)

g. Foreign exchange personnel's performance of assigned duties and functions—to include duty related travel and visits—is administered exclusively in U.S. Army channels and within the scope of the applicable approved job descriptions and DDL.

h. Foreign exchange personnel will not be assigned to DOD contractor facilities.

i. Foreign exchange personnel are required to perform duties outlined in the job description and in the DDL. They are authorized oral and visual receipt of classified information. Access to documentary information required to perform duties will be controlled by the supervisor and designated contact officer. Release of information for retention is not authorized. (This restriction stems from the fact that foreign exchange personnel do not officially represent their parent governments while serving in an exchange capacity.)

j. They may not have unsupervised access to libraries or document catalogs unless the information therein is releasable to the public.

k. Foreign exchange personnel may not have unsupervised access to computer systems (standalone or networked) unless the information accessible by the computer is releasable to their government.

5–31. Access limitations

Foreign exchange personnel access to restricted areas will be in accordance with local policies and procedures and as specified in DDLs, position descriptions, and appropriate agreements. Foreign exchange personnel may not have access to the following types of information:

a. RESTRICTED DATA and FORMERLY RESTRICTED DATA.

b. CMI or CUI provided by another government, department, or agency (including other DOD departments and agencies), unless access is approved in writing by the originating government.

c. Compartmented information, unless authorized by a separate government-to-government agreement.

d. Information bearing a special handling notice or caveat, such as NOFORN, that restricts access, except when authorized by the originator.

e. Any CMI that has not been authorized previously for release by the responsible DA disclosure authority to the exchange professional's government.

5–32. Delegation of Disclosure Letter

Disclosure guidance, in the form of a DDL, will be established for each exchange position. While the foreign disclosure officer (FDO) is responsible for the preparation of the DDL, the DDL's development should be a joint effort between the FDO and the exchange professional's host supervisor. The supervisor should prepare the contents of paragraphs 5 and 6 and the remaining paragraphs should be jointly discussed and agreed to between the FDO and the supervisor. Coordination with the proponent of information to be disclosed and with the FDO is required. DDL will be staffed through command foreign disclosure channels to ODCSINT, DA (DAMI-CIT) for approval. The DDL must contain the information in appendix D.

5–33. Processing nominations of foreign personnel for exchange

a. Only HQDA may approve exchange programs and assignments. On receipt of an administratively acceptable foreign embassy-initiated nomination, ODCSINT will refer the nomination (extended visit request if embassy is on FVS or letter signed by Military Attache) for consideration and confirmation to ODCSOPS for the PEP or HQ AMC for the SEEP. When ODCSINT receives a favorable response from ODCSOPS or HQ AMC, the nomination will then be referred for further consideration and confirmation in command foreign liaison/disclosure channels to the DA agency or MACOM in which the exchange position has been established.

b. The receiving DA agency or MACOM is to—

(1) Examine the nomination carefully to ensure that the nominees's resume of professional experience appears consistent with the qualifications established for the position.

(2) The prospective host DA agency or MACOM must prepare a job description reflecting duties to be performed. The agency or MACOM will prepare a draft DDL to accompany the previous information. (See Appendix D.)

(3) Ensure that exchange personnel are not placed in positions where access is required to CMI not releasable to the parent government, including contingency plans, intelligence information and other sensitive information.

(4) Ensure that the scope and classification level of information proposed for disclosure are the minimum necessary for satisfactory job performance. Additionally, the agency or MACOM must confirm the concurrence of other Army agencies or commands exercising proponent cognizance over the information to be disclosed. Note that all disclosures must be within the scope of existing agreements pertaining to the exchange of information with the exchange officer's parent government. No new disclosure programs or exceptions to the NDP-1 will be considered merely to facilitate the integration of foreign personnel.

(5) Respond to ODCSINT within 30 days indicating its acceptance or rejection of the nominee.

(a) An acceptance response will comply with ODCSINT guidance concerning completion of a DDL, to include but not limited to: detail of job description, recommended level(s) of disclosure, and requisite information on a designated contact officer.

(b) A rejection response is to include sufficient rationale to permit ODCSINT to formulate a definitive explanation to the nominating foreign government or international organization. Because exchange positions are established by formal MOU or MOAs, rejection of a nominee must be based exclusively on the nominee's lack of professional qualifications—or other professional or personal considerations—unless the responding agency or MACOM concurrently notifies the proponent of the MOU, MOA, or program of its desire to cancel or suspend the exchange position.

c. On receipt of the agency's or MACOM's response, ODCSINT will notify the nominating foreign government or international organization of the outcome via FVS if embassy is on line or by letter and will confirm completion of action to all concerned Army elements.

d. Requests for an extension of existing exchange officer's tour of duty will be submitted utilizing an extended visit request format on FVS. Such requests will clearly state under "purpose of visit" the requested new dates and existing visit request number.

5–34. Administering exchange officers

a. Foreign exchange personnel are subject to the same administrative policies and procedures governing their U.S. Army co-workers. Conflicts between the provisions of this and other applicable Army regulations and the language of the governing MOU are to be tentatively resolved in favor of the MOU language, but promptly brought to the attention of appropriate regulation proponents for final resolution.

b. Exchange personnel serve at the pleasure of DA and are expected to conform to the Army's customs and traditions and comply with applicable statutory and regulatory requirements. Formal agreements establishing exchange positions are to contain mutually agreed-upon language governing disciplinary matters. Beyond the provisions of any formal agreement, instances of misconduct are to be reported to ODCSINT, in the manner prescribed in paragraph 5–28f.

c. Foreign exchange personnel must be briefed by their contact officer and FDO and sign a certification similar to the sample in appendix F before being assigned to the host agency. The signed certificate will be maintained by the local foreign disclosure office until the exchange person has departed the assignment.

d. Foreign exchange personnel assigned to positions that might provide access to technical data also must sign a certification governing the rights of the individual and the Department of Defense on inventions and rights in property.

5–35. Temporary duty travel of foreign exchange personnel

a. Travel by an exchange individual, provided the purpose of the travel is within the substntive scope of the individual's approved job description, terms of certification, and are necessary to successful performance of duty, may be approved by the agency or MACOM to which the exchange individual is assigned, subject to the following:

(1) For intra-agency and intra-MACOM travel, proposals are to be coordinated between the contact officer and the servicing foreign disclosure office. Initial coordination may occur in a manner that is mutually acceptable to both parties.

(2) For inter-agency and inter-MACOM travel, agency heads and MACOM commanders will establish suitable internal procedures and administrative requirements.

(3) For HQDA staff elements and their field operating activities; to organizations, installations, and facilities under the jurisdiction of other services; to OSD and DOD agencies; to the Joint Staff (including unified and specified commands); to other Federal agencies; and to commercial firms (for discussions related to items on the U.S. Munitions List), coordination is to be accomplished through foreign disclosure channals. The usual procedure will be to provide a copy of the exchnage individual's DDL. Such requests will only be referred to ODCSINT, DA (DAMI-CIT) for necessary coordination, approval or denial, and notification to all parties concerned only when requested by the proposed recipient or its higher headquarters.

b. For OCONUS travel by CONUS-based personnel, regardless whether travel is to attend a meeting, participate or observe an exercise, or participate in an operation such as DESERT STORM or RESTORE HOPE, provisions of AR 1–40 also are applicable. OCONUS travel by exchange personnel requires approval by the HQDA-level agency responsible for the exchange (such as, ODCSOPS, DA (DAMO-SSF) for PEP and ASARDA (SARD–DI) for SEEP.

c. All travel orders will identify the individual as being on exchange with the U.S. Army.

d. For paragraphs a through c above, determination as to the need for a U.S. escort officer who is from the exchange officer's parent organization and is familiar with the latter's access and limitations. If the prospective host waives the necessity for an escort officer, it will designate a contact officer to supervise the visitor's activities.

e. Proposed travel that does not meet all of the criteria in a, above, is to be referred for action to ODCSINT, DA (DAMI–CIT). Such referrals are to provide full explanations of factors requiring ODCSINT, DA action.

5–36. Supervisor functions

DA officials designated to supervise a foreign exchange person will—

a. Ensure that the persons understand the duties to be performed in the positions to which they are assigned.

b. Ensure that the person is provided access only to that classified and controlled unclassified information necessary to fulfill the duties of the position description as described in the DDL, or as otherwise authorized in writing by the originator.

c. Ensure that coworkers are informed of the limitations on access to information by the exchange person and their responsibilities in dealing with the individual.

d. Inform the foreign exchange person of their obligations, rights, and responsibilities.

e. Ensure that the foreign exchange person signs a certification similar to the sample in appendix F before being assigned to the position.

f. A supervisor who is also the designated contact officer additionally must follow the guidance in paragraph 5–4*c* above.

Chapter 6
Meetings, Conferences and Symposia

Section I
Introduction

6–1. Approval policies

Overall policies governing the approval of, planning for, and conduct of meetings, conferences and symposia (hereafter: "meetings") that are sponsored, cosponsored, or hosted by Army agencies or commands prescribed in various Army regulations (principally AR 380–5 and DODD 5200.12), either by type of meeting or classification of the meeting's contents. This chapter does not alter those policies. With the exception of in-house meetings (see definition in glossary), attendance or participation by foreign representatives at many types of meetings—both classified and unclassified—is a possibility that must be considered and planned for. This chapter is intended to supplement overall policies and to prescribe uniform procedures to accommodate and facilitate foreign attendance or participation, when deemed in the best interests of the Army.

6–2. Types of meetings

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

Section II
Non-Acquisition-Related Meetings

6–3. Established Cooperative Programs

Meetings related to Army participation in established multinational fora relating to doctrinal issues (i.e., personnel, intelligence, operations, logistics, signal, transportation, legal, etc.) are not considered to be acquisitions oriented. If the meeting does not ultimately intend to design, develop, produce, or manufacture materiel or equipment, it falls under this category.

6–4. Unclassified meetings

Cooperative development meetings involving only unclassified information do not require prior approval of ODCSINT; however, attendance of foreign representatives must be requested in the manner prescribed in chapter 5, section II. Integrated members of an international organization such as Headquarters, NATO, or Supreme Headquarters Allied Powers Europe will be authenticated by the U.S. national military representative or U.S. documents officer at the respective headquarters. To facilitate processing of such requests, the Army host or sponsoring organization will notify ODCSINT, DA (DAMI-CIT)—via DA foreign liaison/disclosure channels—of the type, date(s), and locations(s) of the meeting and the identity of the meeting POC (including DSN and commercial telephone number). This information will permit ODCSINT to approve visit requests promptly and notify all concerned parties with little delay.

6–5. Classified meetings

Cooperative development meetings involving the disclosure of classified information to foreign representatives require the designation of a security sponsor and approval by ODCSINT, DA (DAMI-CI). Such approval is to be obtained in the manner prescribed in AR 380-5, chapter 5. This process also notifies ODCSINT to expect foreign RVAs. U.S. attendees at such meetings must understand that neither ODCSINT concurrence in convening the meeting nor ODCSINT approval of related foreign RVAs in any way affects—

a. Each individual's responsibility to obtain approval for information proposed for disclosure at the meeting.

b. The responsibility of the DA sponsor to ensure that all U.S. participants have obtained disclosure authorization for all CMI to be disclosed at the meeting.

Section III
Acquisition-Related Meetings

6–6. Rationalization, standardization, and interoperability

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

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

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

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

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

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

6–7. Planning

Acquisition-related meetings are distinct from other types of meetings in several ways that tend to complicate planning and require special procedures.

a. In some instances, it may be deemed in the Army's best interest to permit attendance by persons who have no government affiliation (i.e., members of the public). In such cases, planners must ensure that all presentations by U.S. citizen personnel have been approved for release to the public in accordance with applicable laws and regulations (e.g., AR 70–31 and AR 360–5 for DA personnel). In all other cases, the substance of the information to be discussed—whether unclassified or classified—requires that attendance and participation at the meeting be limited to those personnel (U.S. and foreign) having official government affiliation or sponsorship and a need-to-know the information to be presented.

b. Eligibility for access to official information, particularly that which is classified, varies from country to country. Accordingly, information to be disclosed at a session attended by foreign representatives will be limited to a level of eligibility (within the required categories set forth in NDP–1) that is common to all foreign representatives at the particular session. It is improper to use special handling markings, such as NOFORN (Not Releasable to Foreign Nationals), that apply to intelligence information (AR 381–1) to control foreign attendance at classified sessions, unless intelligence information will be disclosed and the originating agency specifically determines for the meeting in question that the information is not releasable.

c. When a meeting may lead to the award of a specific contract (e.g., presolicitation, prebidders, preproposal, or preaward meeting), the meeting sponsor or cosponsor must analyze the extent to which classified information may be involved throughout the life cycle of the project. The results of such analysis are prerequisite to a determination of potential foreign involvement in the project and attendance at both unclassified and classified project-related meetings.

6–8. Procedures

After making a preliminary determination to convene or sponsor an acquisition-related meeting that may involve foreign representatives, an Army agency or command is to adhere to the following procedures based on the sensitivity of the information to be disclosed. Figure 6–1 gives a suggested time frame for implementation of the procedure.

a. Unclassified meeting open to the public. Prior ODCSINT approval to convene the meeting is not required; however, the Army sponsor or cosponsor must—

(1) Notify ODCSINT, DA (DAMI–CIT) in the manner prescribed in paragraph 6–4 to facilitate prompt, accurate ODCSINT response to anticipated foreign requests to attend. If the meeting is to be convened in a facility which is not under the jurisdiction of DOD, ODCSINT, DA will consider an Army sponsor's or cosponsor's request to waive requirements for official visit authorization for representatives of foreign countries. If representatives of these countries will attend, it is necessary to obtain HQDA approval for official Army involvement in the event, irrespective of location.

(2) 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 360–5. DOD 5220.22–M, governs presentations by contractor personnel when the information in question is derived from or acquired as a result of a DOD contract. The ITAR or Department of Commerce Export Administration Regulation, as applicable, governs presentations by non-U.S. Government personnel when the information in question is not derived from a DOD contract.

(3) Comply with provisions of AR 70–31 and AR 70–45 regarding the publication and dissemination of meeting proceedings.

b. Unclassified meeting closed to the public. Although prior ODCSINT, DA approval to convene the meeting is not required, the Army sponsor or cosponsor must—

(1) Coordinate with all DA agencies or commands having a proponent or other substantive interest in the subject matter of the meeting to establish attendance criteria for foreign representatives prior to publicizing the meeting. In this regard, it is important to consider the prohibition on false impressions in paragraph 2–2 of this regulation and in DOD 5105.38–M, chapter 5. Rationale for permitting foreign participation must be based on DA involvement in an applicable international activity or project (such as, a bilateral or multilateral cooperative R&D or RSI agreement relevant to the subject matter of the meeting, a reciprocal procurement agreement, or a potential coproduction or co-development plan). When no specific agreement can be identified to allow foreign attendance, the host must judge the benefit to the Army of allowing a particular nation's participation.

(2) Notify ODCSINT, DA (DAMI–CIT) in the manner prescribed in paragraph 6–4, but also include a list of foreign countries whose attendance has been tentatively determined by the DA sponsor to be in the best interests of DA and DOD. This list should include countries to which the Army sponsor desires to issue invitations.

(3) Recall that all non-U.S. Government attendees must—

(a) If U.S. or Canadian citizens certified by the JCO (other than those representing a non-U.S. or non-Canadian interest), be certified by a DOD component as having a bona fide requirement to acquire the information (see AR 70–31).

(b) If foreign citizens (or U.S. or Canadian citizens representing non-U.S. or non-JCO certified Canadian interests), be officially sponsored by a foreign government in the form of a standard RVA (see also para 5–1).

(4) Ensure that all U.S. citizen participants are aware of the requirement to obtain approval for presentations to audiences that contain foreign representatives.

(5) Comply with provisions of AR 70–31 and AR 70–45 regarding the publication and dissemination of meeting proceedings.

c. Classified meeting. AR 380–5 prescribes ODCSINT, DA must approve in advance DA sponsorship of any meeting involving the attendance of foreign representatives and the disclosure of classified information. This requirement also applies to symposia or conferences sponsored or cosponsored by non-Government associations. Because foreign participation in all acquisition-related meetings must be assumed, prior ODCSINT, DA approval is required for all acquisition-related meetings involving the disclosure of classified information. Procedures for obtaining such approval and policies governing the conduct of classified meetings in general are contained in AR 380–5, chapter 5, and are amplified by the following:

(1) Any meeting involving disclosure of classified information to foreign representatives must have a DOD component designated as the security sponsor. Although properly cleared DOD contractors (including associations holding valid facility clearances) may perform security-related administrative functions, they may not be designated as the DOD security sponsors for meetings. Security sponsorship for a classified meeting means that the DOD component has preeminent interest in the subject matter of the meeting, is able to verify the need-to-know of all attendees, and has the authority to approve foreign attendance or participation. Because this combination of characteristics does not exist at echelons below HQDA, a DA agency or commands will not formally agree, on behalf of HQDA, to serve as the DOD component security sponsor for a classified meeting without the prior written authorization of ODCSINT, DA (DAMI-CIS), obtained in the manner prescribed in AR 380–5, chapter 5. Associations approaching a DA agency or command to arrange for a meeting may give the impression either that the event has been fully sanctioned by DOD or that the association (or a cleared contractor member of the association) is prepared to accept total responsibility for obtaining necessary DOD approval for the meeting and arranging all security-related aspects. DOD policies, however, strictly prohibit such actions by cleared contractors or associations acting on their behalf.

(2) A DA agency or command is not authorized to agree to host (as opposed to sponsor) a classified meeting without prior written verification from ODCSINT, DA (DAMI–CIS). The verification will confirm whether another DOD component has accepted formal security sponsorship for the meeting on behalf of DOD.

(3) A request for approval to serve on behalf of DA or DOD as the security sponsor for a classified acquisition-related meeting is to be addressed in command security/foreign disclosure channels to ODCSINT, DA (DAMI–CIS). The request must arrive at ODCSINT, DA no later than 120 days prior to the meeting date and contain the following:

(a) Subject and title of the meeting, a topical outline (including security classification of each topic, originating authority or agency of the information proposed for release, and verification that the topics have been cleared for release to the nations planned to be invited to the conference), and a statement supporting the agency's or command's preeminent interest in the meeting's subject matter.

(b) Date and specific U.S. Government installation or cleared U.S. contractor location of the meeting.

(c) Identity of the person designated to be the agency or command POC for arranging the meeting and the person designated to be the security manager for the meeting. Name, grade, and telephone number must be included.

(d) Name and contact person of any cosponsoring non-Government association involved.

(e) List of foreign countries to which the prospective sponsor wishes to send invitations, or from which requests to attend or participate may be expected (with supporting rationale for such participation).

(f) If applicable, and in lieu of (3) above, a fully justified proposal to totally exclude otherwise eligible foreign attendees or participants from the meeting in its entirety. Rationale for total exclusion must be based primarily on the grounds of national security, be consistent with current national disclosure policies, and reflect an assessment of the meeting's total content. It is important to note that individual presentations—or topics as a whole—deemed unsuitable for release to all potentially eligible attendees can frequently be modified to a suitably releasable form, or may be presented at one or more sessions of the meeting designated for U.S. personnel only. Justification must also include description of the information or technology that must be protected, a discussion of the U.S. lead in technology that serves as the purpose for exclusion, and a statement affirming that no international agreements would be adversely affected by exclusion. Each request should be staffed with both intelligence and multinational program offices of the requesting command prior to submission.

(4) On receipt of the foregoing request for sponsorship approval, ODCSINT, DA will coordinate with relevant HQDA and OSD staff elements and respond to the requester within 10 working days. If sponsorship is approved, the ODCSINT response will contain—

(a) A list of eligible foreign countries for which attendance or participation would be approved on formal foreign government request. This information eases planning (including dispatching of invitations) and preparation of presentations.

(b) A statement summarizing foreign attendance eligibility criteria—for incorporation in publicity for the meeting.

(5) The approved DA security sponsor is responsible for ensuring that each person scheduled to give a presentation at the meeting is informed of foreign countries expected to have representatives in attendance and of his or her responsibility to—

(a) Submit an abstract or detailed outline of the presentation, for preliminary disclosure review and guidance, in relevant command security/foreign disclosure channels. This abstract or outline is to arrive at the first level of command or technical supervision exercising disclosure authority within 30 days following notification. A non-Army cosponsor (such as, an industrial association) may collect and submit abstracts or outlines to ODCSINT, DA (DAMI–CIT) in bulk, for further dissemination.

(b) Submit a copy of the final text of the presentation (and any supporting graphic aids) for formal disclosure determination in established command security/foreign disclosure channels to the applicable DA agency or MACOM exercising disclosure authority. This copy must arrive no later than 45 days prior to the meeting (60 days if the information involves proprietary restrictions or is of third-country origin). A disclosure determination normally will not be rendered on graphic aids in the absence of an accompanying briefing text. Obtaining disclosure authorization is the exclusive responsibility of the individual proposing to render the presentation. DA contractor personnel should be referred to procedures prescribed in DOD 5220.22–M, paragraphs 5.q. and 9.e.

(6) ODCSINT, DA will approve or deny official foreign government requests for meeting attendance or participation on receiving them, but not later than 30 days prior to the meeting. When the Army's best interest would be served, and when additional attendance/participation would not alter the meeting's composition or previous disclosure determinations, ODCSINT, DA reserves the option to accept and approve requests not received on time.

(7) The DA security sponsor is to ensure compliance with provisions of AR 70–41 and AR 70–45 regarding the publication and dissemination of meeting proceedings.

(8) Other responsibilities of the DA security sponsor's designated meeting security manager are as follows:

(a) Ensure that attendance is limited to U.S. and foreign government and industry representatives whose security clearances and need-to-know have been established to the satisfaction of the DA sponsor or cosponsor.

(b) Ensure that each presentation to be rendered—whether classified or unclassified—has been duly approved in writing for disclosure to the countries represented by the foreign personnel in attendance. Prohibit presentations that do not bear evidence of proper approval.

(c) Advise both U.S. and foreign attendees of the consequences of unauthorized dissemination of information disclosed at the meeting.

(d) Control the taking of notes during classified presentations.

(e) Ensure that areas in which classified presentations are to be rendered are properly cleared for such use.

(f) Provide facilities for the temporary storage of classified materials.

(g) Ensure that proceedings of the meeting are properly published, marked, and disseminated in accordance with AR 70–31 and AR 380–5.

(h) Promptly report known or suspected security violations to ODCSINT, DA (DAMI–CIT).

Figure 6–1. Guidelines for foreign participation in classified meetings

1. Step 1—8 months prior to the meeting

Association or host command must approach Defense technical representatives to identify topics to be covered and probable classification level of information involved for planned meeting, conference, or symposium in accordance with AR 380–5.

2. Step 2—7 month prior to the meeting

Association or host command must coordiante with local FDO and through command channels to HQDA foreign disclosure representatives to—

a. Determine countries that can potentially attend, based on topics to be covered and classification level and sensitivity of information involved, or request to exclude otherwise qualified foreign industry representatives from participation.

b. Identify host and Army security manager. Army activity sponsoring classified meeting will be reponsible for all supporting security requirements for conference.

c. Select meeting site. Classified meetings will be held only at Government installations or cleared DA contractor facilities in which adequate safeguards can be applied.

d. Draft properly formulated limiting statements for inclusion in advertising literature. Notices or invitations to attend classified meetings will be sent only to appropriately cleared personne.

3. Step 3—6 months prior to the meeting

Association or host command will develop call for papers, including disclosure guidelines for the meeting, information on anticipated foreign attendance, and instructions on obtaining written disclosure authorization from the proponent for materiel to be presented. This written authorization must include specific countries to which the paper can be disclosed. (Physical transmittal of any classified information must be authorized in advance.)

4. Step 4—3 months prior to the meeting

Association or host command provide copies of unclassified abstracts of potential papers for foreign disclosure review by the FDO. Each abstract should include title of paper, full name and position of author or authors, name of company or organization represented, and name of DA information proponent agency, if applicable. If release determination cannot be made, abstract should be sent to ODCSINT, DA (DAMI–CIT) for processing.

5. Step 5—2 months prior to the meeting

Papers prepared by US Government and military personnel will be submitted through originating command-level security and foreign disclosure office to appropriate MACOM for approval or futher coordination. Papers prepared by US industry, educators, and other non-Government personnel willbe submitted through appropriate Government contract program office for clearance if no approved munitions license exists. If information to be released is covered by approved munitions license, caution must be exercised to ensure terms of license include all potential foreign participants at symposium.

Appendix A
References

Section I
Required Publications

AR 1–40
Clearance Requirements and Procedures For Official Temporary Duty Travel Outside Continental United States. (Cited in paras 4-2a(2) and 5-36b.)

AR 34–1
International Rationalization/Standardization and Interoperability. (Cited in paras 1-20, 2-11a, 3-6, 3-7a(1), and 3-8b(1).)

AR 70–11
Dissemination of Scientific and Technical Information. (Cited in paras 4-6a(1) and 4-8d.)

AR 70–31
Standards for Technical Reporting. (Cited in paras 2-8, 2-10, 3-4a, 4-6a(1), and 6-8b.)

AR 70–33
Mutual Weapons Development Data Exchange Program (MWDDEP) and Defense Development Exchange Program (DDEP). (Cited in paras 1-20, 2-11, and 3-8b.)

AR 70–41
Cooperation With Allies and Other Nations in Research and Development of Defense Equipment. (Cited in paras 2-11c, 3-8b(2), 3-9a, and 6-8c(7).)

AR 70–58
International Professional (Scientists and Engineers) Exchange Program. (Cited in para 3-8c.)

AR 380–5
Department of the Army Information Security Program. (Cited in paras 4-2b(1), 4-9b(1), 5-19, 6-1, 6-5, and 6-8c(8)(g).)

AR 380–15 (C)
Safeguarding Classified NATO Information (U). (Cited in para 5-20a.)

AR 381–1
Security Control of Dissemination of Intelligence Information. (Cited in para 6-7b.)

AR 381–12
Subversion and Espionage Directed Against the U.S. Army (SAEDA). (Cited in para 5-6.)

AR 550–51
Authority and Responsibility for Negotiating, Concluding, Forwarding, and Depositing of International Agreements. (Cited in para 2-11a, 2-11c, 2-11e, 3-1a, 3-9a, 5-29.)

AR 614–10
US Army Personnel Exchange Program With Armies of Other Nations; Short Title: Personnel Exchange Program. (Cited in paras 3-8c, and 5-29b.)

Section II
Related Publications

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

AR 12–1
Security Assistance - Policy, Objectives, and Responsibilities

AR 12–8
Security Assistance - Operations and Procedures

AR 12–15
Joint Security Assistance Training (JSAT) Regulation

AR 25–55
The Department of the Army Freedom of Information Act Program.

AR 25–400–2
Modern Army Record Keeping System

AR 40–3
Medical Dental and Veterinary Care

AR 70–1
Systems Acquisitions Policy and Procedures

AR 70–57
Military-Civilian Technology Transfer

AR 95–1
Army Aviation: Flight Regulations

AR 210–50
Housing Management

AR 340–21
The Army Privacy Program

AR 360–5
Army Public Affairs, Public Information

AR 380–28 (C)
The Department of the Army Special Security System (U).

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

AR 525–16
Temporary Cross-Border Movement of Land Forces Between the United States and Canada

AR 530–1
Operations Security

DoD 5105.38–M
Security Assistance Management Manual

DoD 5200.1–R
Information Security Program Regulation

DoD 5220.22–M
Industrial Security Manual for Safeguarding Classified Information

DoDD 2040.2
International Transfers of Technology, Goods, Services, and Munitions

DoDD 5000.1
Defense Acquisition

DoDD 5100.55
United States Security Authority for North Atlantic Treaty Organization Affairs

DoDD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations

DoDD 5230.20
Visits and Assignments of Foreign Representatives

DoDD C-5230.23
Intelligence Disclosure Policy (U)

DoDD 5230.24
Distribution Statements on Technical Documents

DoDD 5230.25
Withholding of Unclassified Technical Data From Public Disclosure

DoDD 5400.7
DoD Freedom of Information Act Program

DoDI 5000.2
Defense Acquisition Management Policies and Procedures

DoDI C-5220.29
Implementation of the North Atlantic Treaty Organization Industrial Security Procedures (U)

DoDI 5230.18
The DoD Foreign Disclosure and Technical Information System (FORDTIS)

EAR
Export Administration Regulations (15 C.F.R. 368-399)

MCTL
Militarily Critical Technologies List

NDP-1 (S)
National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations. (Copies of this publication may be obtained from HQDA (DAMI-CIT) WASH DC 20310-1057.)

US-Canada Joint Certification Program. OUSD(P) Pamphlet

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Form 39 (C)
Document Accountability Record

DD Form 441
Department of Defense Security Agreement

DD Form 1822
Report of Disclosure/Denial of US Classified Military Information

DD Form 2345
Militarily Critical Technical Data Agreement

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

Section V
Recordkeeping Requirements

This regulation requires the creation, maintenance, and use of the following specific records. (See app B of AR 25-400-2 for file numbers descriptions, and dispositions.)

FN 380-10a
Systems and materials

FN 380-10b
Country files

FN 380-10c
Technology transfer cases

FN 380-10d
Foreign national visits

FN 380-10e
Foreign representative certifications

FN 380-10f
Foreign military attache files

FN 380-10g
Foreign national protocol files

FN 380-10h
Foreign national tours

Appendix B
Exceptions to Policy

B-1. Exceptions to the National Disclosure Policy (NDP-1)

a. An exception to NDP-1 (ENDP) is required when a potential disclosure of CMI—

(1) Exceeds NDP-1-prescribed maximum classification level for which the prospective foreign government or international organization recipient is eligible within the CMI category in question.

(2) Does not conform to any of the basic disclosure criteria and conditions prescribed by NDP-1 and listed in paragraph 2-4.

b. Each proposed ENDP is to be sponsored by the HQDA staff agency designated in chapter 1, section II, para 2-11 of this regulation as exercising primary delegated disclosure authority for the category of CMI that is predominant in the matter at issue. The sponsoring agency is to--

(1) Obtain ARSTAF and cognizant functional OSD office concurrence in seeking the ENDP.

(2) Task appropriate agencies to provide the complete requisite supporting rationale or justification to ODCSINT, DA (DAMI-CIT).

(3) Formally request that ENDP be initiated by ODCSINT, DA (DAMI-CIT).

c. ODCSINT, DA (DAMI-CIT) will—

(1) Prepare the proposed ENDP in final form, as depicted in figure B-1.

(2) Coordinate the final ENDP package with the sponsoring HQDA agency prior to submission to the NDPC.

B-2. Exceptions to DA policy

a. An exception to DA policy is required whenever a potential disclosure of CMI or CUI does not conform to policies or procedures established in this regulation.

b. Requests for exceptions to DA policy—

(1) May be submitted by an DA agency or command.

(2) Are to be submitted in command foreign disclosure channels.

(3) Are to be prepared and submitted in letter form, unless the urgency of need necessitates submission in electrical message form.

(4) Are to incorporate applicable elements from figure B-1.

Figure B–1. Format for a Request for Exception to the NDP

DAMI-CIT (380-10c) *(Date)*

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

SUBJECT: Request for Exception to the National Disclosure Policy (E-NDP) --*(Insert country here)* (Army NDPC Case Nr. 2000-00) (U)

1. (U) The Department of the Army requests *(insert either "a continuing" or "a one-time")* exception to the National Disclosure Policy to permit the disclosure of *(insert CLASSIFICATION) (insert one or more NDP categories, each with its designation, e.g., "Category 1, Organization, Training, and Employment of Military Forces")* information to the Government of *(insert country)* (remainder of sentence states very concisely why the exception is being requested, e.g., ''in furtherance of the possible sale of the (system) to the *(country)* armed forces'' or ''in support of the negotiation of a Data Exchange Agreement pertaining to *(system)*'')

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

3. (U) An assessment of how each of the disclosure criteria and conditions set forth in section II (Policy) of NDP-1 (as well as Chapter 1, C-1.a., of this regulation) will be met as follows:

a. (U) Disclosure is consistent with the foreign policy of the United States toward the Government of *(the recipient government)*. (Cite these policies or objectives, avoiding generalities such as ''the recipient cooperates with the United States in pursuance of military or political objectives.) The JCS ''Joint Strategic Planning Document Supporting Analysis (JSPDSA)'' is a good source document for this entry. ODCSOPS POL-MIL and ODCSINT Foreign Intelligence Division can provide information to support or validate this justification.)

b. (U) The military security of the United States permits disclosure. Disclosure of advanced technology, if compromised, will not constitute an unreasonable risk to the US military technology. (Explain. Describe the system. Designate exactly what you are trying to sell or release. What components are classified? What elements are really critical? Does the system or do its components represent a significant advance in the state-of-the-art? What other countries have this system? Are comparable systems (foreign or domestic) using the same technology already in the marketplace? What precedent exists for release of this particular system? Are export versions available? Do the program manager (PM) and OASA(RDA) support the release of this system? If there is a security classification guide for this system, it should be attached as an enclosure.)

c. (U) 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. This statement is supported in part by the following:

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

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

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

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

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

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

d. (U) Disclosure will result in benefits to the United States at least equivalent to the value of the information disclosed.

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

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

(3) (U) (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. (U) 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 preparer should indicate clearly that release of R&D (Category 3) or Production (Category 4) data is not involved or that documentation will be sanitized.)

4. (U) (Explain any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure schedules, or other pertinent caveats that may affect approval or denial of the request. Limitations are developed working with ASA(RDA), the PM, or both. Limitations include phasing of the release, substitution or removal of components, prohibitions on the release of certain hardware or information, and restrictions that must be included before the release can be executed. It should be

Figure B–1. Format for a Request for Exception to the NDP—Continued

noted that if there is no security agreement in force, an item-specific agreement must be executed with the recipient country before the release.)

5. (U) The requested exception is a continuing exception, subject to annual review (or ''is a one-time exception to expire on'' a given date). (A continuing exception usually is associated with a long-term project, such as a coproduction program or military sale when the United States will be obligated to provide life cycle support. A one-time exception typically is used for a briefing or demonstration or short-term training.)

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

7. (U) (Add here the opinion of other interested Departments or Agencies if joint-Service or shared information is involved. If the information or item of equipment is of shared or joint interest, such as an air-to-air missile used by two Services or containing technology of concern to another Service, the views of the other party should be included.)

8. (U) (Add here any information not mentioned that would assist the NDPC members, the Secretary of Defense, or the Deputy Secretary of Defense in evaluating the proposal. The preparer can use this paragraph to present evidence that would counter arguments (usually involving the security status of the proposed recipient or concerns for the technology involved) opposing the release. The preparer must not attempt to hide these opposing views but must address each issue. Failure to do so may result in an adverse reaction to the case when these issues are eventually raised.)

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

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

b. (U) *(Name, rank (if military)*, office symbol, and telephone number of the PM, Office of the Deputy Chief of Staff for RD&A official, and technical expert on the system at issue, as applicable.)

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

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

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

Encls

Signature Block
LTC, GS
Army Member, NDPC

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

Appendix C
Technology Assessment/Control Plan (TA/CP)

C–1. Overview

a. The TA/CP requirements set forth in paragraphs C-1 through C-4 below meet the technology assessment prerequisite for requests for authority to negotiate (RAN) an international agreement. In developing the TA/CP, cognizant DOD Components will consider and incorporate, as appropriate, all applicable National Disclosure Policy (NDP) and DOD technology transfer policy guidelines, and service disclosure policy.

b. After OSD review, the TA/CP will be used by the cognizant DOD Component as the basis for developing negotiating guidance prior to negotiations with a foreign government.

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

d. The DDL also will provide specific and detailed guidance to support evaluation of proposed exports/releases of defense articles and technical documents by DOD Components and defense contractors. The attached format may be used as general guidance for preparation of DDLs.

e. Upon conclusion of an agreement, the DDL will be updated as required and issued by the participating DOD Component to ensure that transfers of defense articles and information by US government or US industry personnel will comply with the TA/CP, NDP, and applicable DOD/Service security policies and procedures.

C–2. Program concept

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

C–3. Nature and scope of effort/objectives

State the operational and technical objectives of the proposed program. Indicate specifically the following:

a. Nature and scope of the activity (for example, cooperative research, development, and/or production).

b. Country or country groups participating, and the anticipated extent of participation by each, including identification of foreign contractors and subcontractors, if known. Differentiate between those that are committed participants and those that are only potential participants.

c. Program phases involved and, if applicable, quantities to be developed and produced or tested.

d. Summary of projected benefits to United States and other participants: technology, production bases, and military capability (detailed in para C-3*e* below).

e. Cognizant POCs within DOD Component headquarters or program management organization.

f. Major milestones or dates by which the assessment will require review or revision.

C–4. Technology assessment

a. Identify products or technologies involved in the program. This section of the assessment should discuss topics listed below using the MCTL and other applicable DOD technology transfer policies as guides.

(1) Design and manufacturing know-how and equipment used for development and production.

(2) Systems or components or information used for other purposes (for example maintenance or testing) that would allow a recipient to achieve a major operational advance. (When applicable, cite other specific US programs and projects from which technical information or hardware will be provided.)

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

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

(1) Current or projected capabilities worldwide;

(2) Current or projected capabilities of proposed participants or recipients; and

(3) Availability of technologies worldwide.

d. Identify any previous releases or current programs (such as sales, cooperative programs, information exchange) involving the transfer or exchange of this or comparable equipment and technologies.

e. Describe the impact on US and foreign military capability as a result of participation in this program:

(1) Identify and describe the extent to which the US system or technology contributes to an advance in the state of the art, or a unique operational advantage. Include, if known, a summary of US investment and R&D or operational lead-time represented.

(2) State the specific contribution of foreign participants to program objectives, project resources, and enhancement of the US military capability and technology base.

f. Describe the potential damage to the US technology position and military capability in the event of a compromise (without regard to potential participants). Explicitly address the impact of loss or diversion of the system or technology. Specify assumptions and discuss the following:

(1) Transfer of a military capability the loss of which would threaten US military effectiveness (for example a missile seeker for which we have no countermeasures, or information allowing the development of effective countermeasures negating a primary US technological advantage).

(2) Potential compromise of sensitive information revealing systems' weaknesses that could be exploited to defeat or minimize the effectiveness of US systems;

(3) Susceptibility to reverse engineering of sensitive design features or fabrication methods;

(4) Extent to which the technology that is to be transferred can be diverted and/or exploited for purposes other than the one intended under the specific program (e.g., a technological capability to fabricate ring laser gyros translates into an ability to implement advanced long-range missiles, precision land and sea navigation, etc.); or

(5) Potential impact of participation on US competitive position or US industrial base, if any. (The conclusions of the Industrial Base Factors Analysis may be incorporated by reference.)

g. Estimate the risk of compromise, considering the following:

(1) Susceptibility of the technology to diversion or exploitation, and its priority as a target for foreign intelligence service (FIS) collection, if known. (The degree of susceptibility will depend to a great extent on the exact nature of the technology in question, the form of the transfer, and the indigenous capability of the recipient);

(2) The potential participants/recipients, including:

(a) An evaluation of their security and export control programs (including reference to any specifically related agreements with the US).

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

C–5. Control plan

This section of the TA/CP is the basis for negotiating guidance for agreements, and ultimately will be implemented in the DDL. Specifically, this section will identify measures proposed to minimize both the potential risks and damage due to loss, diversion, or compromise of the critical/ classified elements identified in sections C-3a and b above, and will clearly identify any specific limitations/conditions required to protect unique US military operational and technological capabilities. Appropriate measures that should be considered and discussed include:

a. Phased release of information to ensure that information is disseminated only when and to the extent required to conduct the program. (Specifically, production technology should not be released prior to a program decision requiring the use of the technology in question.);

b. Restrictions on releases of specific information to protect US national security interests. Be specific with regard to details of design and production know-how and software, including software documentation, development tools and know-how;

c. Release of specific hardware or software components in modified form, or as completed, tested items;

d. Special security procedures (both government and industrial) to control access to restricted materiel and information. Also to be considered are:

(1) Controls on access of foreign nationals at US facilities; and

(2) Procedures to control releases by US personnel at foreign facilities; and

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

C–6. Notes

a. In some cases, particularly early in R&D programs, the full range of technological alternatives and potential participants may not be fully known. Specific hardware and technical data may not be completely defined, and the nature and availability of end items and technical data can evolve rapidly during a development program. In these cases the TA/CP should define comprehensive technical criteria, in sufficient detail to support release decisions as the program evolves.

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

c. TA/CPs and other technology security related documents often contain classified or controlled unclassified information of a sensitive nature. These documents should have distribution statements applied to preclude unauthorized public disclosure or disclosure to inappropriate entities.

Appendix D
Delegation of Disclosure Authority Letter (DDL)

The following DDL formats (figs D-1 and D-2) should be used by DA elements. All items identified will be provided in the order shown. Each DDL requires a warning statement which, as a minimum, is to be placed at the top of the DDL;s first page and the bottom of the last page. It is recommended it be placed at the top of each page. It must be bold and in larger letters than the DDL;s contents so it clearly stands out. The wording of the warning statement is below.

Figure D–1. DDL for weapons system or data exchange annexes

EXAMPLE 1

Delegation of Disclosure Authority Letter for Weapons Systems or Data Exchange Annexes (DEA's)

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

OFFICE SYMBOL (380-10)

SUBJECT: Delegation of Disclosure Authority Letter (DDL)/**DA ASSIGNED NUMBER**

TITLE: Delegation of Disclosure Authority Letter..**INDICATE COMMAND RECEIVING AUTHORITY**

I. CLASSIFICATION: The highest level of military information that may be disclosed is... **INDICATE HIGHEST SECURITY CLASSIFICATION LEVEL AUTHORIZED FOR RELEASE.**

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

3. CATEGORIES PERMITTED: USING TABLE 2 AS A GUIDE, INDICATE THE CATEGORIES OF INFORMATION AUTHORIZED FOR RELEASE.

4. SCOPE: INDICATE CLEARLY TO WHOM THE DISCLOSURE AUTHORITY IS GRANTED, FOR WHAT PROGRAM, SYSTEM, STUDY ETC, AND CLEARLY INDICATE THE AUTHORIZED RECIPIENT(S). INDICATE WHAT AGREEMENTS, MOA'S, DEA'S, FMS CASES, INTERNATIONAL COOPERATIVE PROGRAMS ARE INVOLVED. As an example: The Commander MICOM is delegated authority to disclose CMI originated by MICOM within the categories listed in paragraph 3, subject to the limitations delineated in paragraphs 5 and 6. The Commander may also disclose CMI originated outside of MICOM when the disclosure is authorized by the originator of the information to:

United Kingdom of Great Britain and Northern Ireland
Republic of France
Federal Republic of Germany

IN THIS PARAGRAPH BE AS COMPLETE AND AS DESCRIPTIVE AS POSSIBLE TO ENSURE A COMPLETE UNDERSTANDING BY HQDA. INCOMPLETE OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS AT HQDA OR THE RETURN OF THE DDL FOR REWRITE.

5. AUTHORIZED FOR RELEASE/DISCLOSURE: IN THIS PARAGRAPH IT MUST BE CLEARLY STATED WHAT INFORMATION UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY IS/WILL BE AUTHORIZED FOR RELEASE. IT IS IMPORTANT THAT THE DDL DEVELOPING AUTHORITY BE AS DETAILED AS POSSIBLE IN OUTLINING PORTIONS OF PROGRAMS, SYSTEMS, STUDIES, ETC. THAT THIS DDL IS DESIGNED TO COVER. THIS PARAGRAPH SHOULD PROVIDE SPECIFIC DETAILS REGARDING THE INFORMATION TO BE RELEASED, TO INCLUDE THE LEVELS OF THE CLASSIFICATION ANTICIPATED FOR RELEASE AT DIFFERENT PHASES OF THE PROGRAM. TERMINOLOGY USED MUST BE CONSISTENT WITH THAT USED IN THE DEVELOPMENT OF THE APPLICABLE SYSTEM SECURITY CLASSIFICATION GUIDE (SCG). THE SCG'S FOR A WEAPONS SYSTEMS OR TECHNOLOGY PROVIDE A COMMON LANGUAGE AND FRAMEWORK FOR DEVELOPING PARAGRAPH 5 AND 6. IT IS RECOMMENDED THAT THE LANGUAGE IN THE GUIDES AS WHO'LL AS THE TOPICAL SUBDIVISIONS IN THE GUIDE BE USED AS A TEMPLATE FOR STRUCTURING YOUR PARAGRAPH 5 AND 6. INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS AT HQDA AND THE RETURN OF THE DDL FOR REWRITE. For example:

WEAPONS SYSTEM PERFORMANCE AND CAPABILITIES

(a) Projectile: Analysis data relative to the projectile, specifically

(b) Submunition: Countermeasures related to the submunition, specifically

6. NOT AUTHORIZED FOR RELEASE/DISCLOSURE: THIS PARAGRAPH MUST SPECIFY THE LIMITS OF THE DISCLOSURE AUTHORITY. INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS AT HQDA AND/OR THE RETURN OF THE DDL FOR REWRITE. AS A MINIMUM THE FOLLOWING INFORMATION SHOULD BE INCLUDED: The following CMI is not authorized for release or disclosure under the terms of this DDL. Requests for exception to these restrictions must be forwarded through foreign disclosure channels to HQDA.

a. GENERAL:

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

Figure D–1. DDL for weapons system or data exchange annexes—Continued

Information under the cognizance of another Military Department.

Propriety information owned by a private firm or citizen.

Information obtained form a foreign government unless the foreign government authorizes the disclosure to a third party. The authorization must be in writing.

Data which carries any caveats or markings which limit access.

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

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

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

Low Observable requirements or Advanced Signatures Data.

Non-Cooperative Recognition Data.

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

b. SPECIFIC: SPECIFIC ITEMS LISTED AS NOT AUTHORIZED FOR RELEASE MUST BE INDICATED AT THE SAME LEVEL OF DETAIL AS IN PARAGRAPH 5 ABOVE. INFORMATION THAT WAS CLASSIFIED UNDER THE ORIGINAL CLASSIFICATION AUTHORITY OF AN INDIVIDUAL/AGENCY OTHER THAN THE DELEGATION AUTHORITY SPECIFIED IN THIS DDL IS NOT AUTHORIZED FOR RELEASE WITHOUT THE WRITTEN APPROVAL OF THAT INDIVIDUAL/AGENCY. PARAGRAPH 7 PROVIDES PROCEDURES FOR DISCLOSURE OF CMI NOT UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY LISTED IN THIS DELEGATION OF DISCLOSURE AUTHORITY LETTER.

***7. PROCEDURES:* THE FOLLOWING INFORMATION (BUT NOT LIMITED TO) MUST BE INCLUDED IN THIS PARAGRAPH:** The following procedures will be followed concerning the disclosure or denial of CMI authorized under the terms of this DDL.

a. All CMI disclosures or denials will be consistent with this DDL, comply with the 'need to know' principle, and will take into account the level of foreign **(IDENTIFY)** government in the.. **(LIST PROGRAM, STUDY, SYSTEM INVOLVED).** Classified disclosure will be limited to the minimum level of classification and detail necessary to accomplish the specific purpose of the disclosure.

b. Classified documents will be released to foreign **(IDENTIFY)** representatives only through government to government channels.

c. Transfer of classified documents to foreign **(IDENTIFY)** government representatives will be processed through **(CLEARLY DEFINE APPROPRIATE FOREIGN DISCLOSURE CHANNELS)** i.e. the Security Division, Installation Support Activity. Documents will be forwarded to directly to the foreign **(IDENTIFY)** embassy or provided to a duly authorized representative of the receiving **(IDENTIFY)** government such as an LNO **(IDENTIFY, i.e UK LNO certified to HQ TRADOC).**

d. Records of Disclosure or Denial of Classified Military Information:

(1) Authorized representatives **(IDENTIFY BY TITLE OR POSITION WITHIN THE COMMAND)** who disclose classified information (oral, visual, documentary) to foreign **(IDENTIFY)** officials **WILL** record the disclosure (using DD Form 1822, Report of Disclosure or Denial of US Classified Information) and forward the record to the nearest supporting foreign disclosure office,. **(SPECIFY WHERE THE DISCLOSURE RECORD *IS TO BE FORWARDED, i.e.* SECURITY DIVISION, INSTALLATION SUPPORT ACTIVITY, ETC)** when one of the following occurs:

(a) First time disclosures based on one of the following: new information, new (higher) classification level, or new (country) recipient. Examples are:

1. The first time we disclose information to Country Z, it must be recorded. There is no need to re-record the disclosure every time we disclose **the same information** to Country Z.

2. Suppose the original disclosure to Country Z was at the Confidential level. Now we have new/additional information on the same subject but the new information is classified Secret. If we disclose the new information to Country Z, this must be recorded as it is at a new (higher) classification level.

3. Suppose we have disclosed Confidential information to Country Z. Now we obtain authority to disclose it to Country Y. The second disclosure must be recorded as there is a new (country) recipient.

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

1. Suppose we wish to tell Country Z for the first time there are Country Y military personnel training in the adjoining nation. The information is classified. We record this disclosure. Later we wish to tell Country Z that the number of military personnel Country Y has training in the adjoining nation is 200 and they are part of an armor unit. The second proposed disclosure is also classified and modifies or extends the scope of the original information. The level of classification for both (whether the same or different) is not critical here. What is important is what we propose to disclose extends the scope of the original disclosure. Therefore, if we do disclose the second information to Country Z, it needs to be recorded.

2. Suppose we tell Country Z for the first time about some classified capabilities of our newest helicopter. We record this disclosure. Later we find it to our benefit to tell Country Z about more or all of the classified capabilities of our newest helicopter. The level of classification for both (whether the same or different) is not critical here. What is important is what we propose to disclose extends the scope of the original disclosure. Therefore, if we do disclose the capabilities to Country Z, that disclosure needs to be recorded.

The authorized disclosing representatives will ensure that all disclosures fitting any of the above categories and within the terms of this DDL are reported using the DD Form 1822

(2) The Security Division, Installation Support Activity **WILL** enter the disclosure into the Foreign Disclosure and Technical Information System (*FORDTIS*) data base.

(3) If a FORDTIS terminal is not available, the DD Form 1822 will be checked for completeness by the supporting Security Division, Installation Support Activity and forwarded to MACOM level for entry into FORDTIS. Instructions for data entry are in DOD 5230.18M, The Foreign Disclosure and Technical Information Systems Users Manual.

e. Army originated CMI not under the classification authority designated in this DDL may be disclosed with the approval authority (in writing) of the designated foreign disclosure authority at the MACOM **(IDENTIFY)** level. MACOM **(IDENTIFY)** level disclosure authorities will coordinate directly with appropriate MACOM's or MACOM equivalents on the disclosure of CMI to support this DDL.

f. CMI under the cognizance of another military department or defense agency will be forwarded through foreign disclosure channels to HQDA for coordination and approval of disclosure.

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

Figure D–2. DDL for liaison officer and exchange officer

EXAMPLE 2

Delegation of Disclosure Authority Letter for Liaison Officer, Exchange Officer, and Scientific and Engineer Exchange Program positions

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

OFFICE SYMBOL (380-10) (DATE)

SUBJECT: Delegation of Disclosure Authority (DDL) for **(IDENTIFY BY NAME AND COUNTRY)** such as: LTC John Doe, British National **/DA ASSIGNED NUMBER**

TITLE: Delegation of Disclosure Authority Letter for...**INDICATE COMMAND RECEIVING AUTHORITY.**

1. CLASSIFICATION: The highest level of military information that may be disclosed is... **INDICATE HIGHEST SECURITY CLASSIFICATION LEVEL AUTHORIZED FOR RELEASE.**

2. DISCLOSURE METHODS: INDICATE TYPES OF DISCLOSURE METHODS AUTHORIZED. There are two types: (1) Oral and visual and (2) documentary. Documentary means the physical transfer of information to a foreign government. PEPs are limited to "oral and visual" because they do not represent their government. LNOs represent their government and if authorized in writing by their embassy, may be given CMI authorized for transfer to their government in lieu of mailing the information to the embassy.

3. CATEGORIES PERMITTED: USING TABLE 2 AS A GUIDE. INDICATE THE CATEGORIES OF INFORMATION AUTHORIZED FOR RELEASE.

4. SCOPE: INDICATE CLEARLY TO WHOM THE DISCLOSURE AUTHORITY IS GRANTED, FOR WHAT PROGRAM, SYSTEM, STUDY ETC, AND CLEARLY INDICATE THE AUTHORIZED RECIPIENT(S). INDICATE WHAT AGREEMENTS, MOUs, DEAs, FMS CASES, INTERNATIONAL COOPERATIVE PROGRAMS, INSTALLATIONS, AND/OR AGENCIES THAT THE INDIVIDUAL(S) WILL, IN THE NORMAL COURSE OF DUTIES, DEAL WITH FOR THE DURATION OF HIS TENURE IN THIS POSITION. As an example: The Commander, US Army Missile Command is delegated authority to disclose classified military information (CMI) within the categories listed in paragraph 3 for the Top Dart Missile Program to:

John M. Doe, Major, Army
United Kingdom of Great Britain and Northern Ireland
UK Liaison Officer, Top Dart Program
Assigned to: US MICOM **(THIS IS COMMAND/AGENCY TO WHICH EXTENDED VISIT IS AUTHORIZED)**

Associated Installations/Agencies/Commands: White Sands Missile Range, NM; Ft. Bliss, TX; AYX Corporation, New York, NY **(THESE ARE INSTALLATIONS, ETC THAT THE INDIVIDUAL WILL VISIT ON A ROUTINE BASIS AS A RESULT OF HIS DUTIES AND TO WHICH THE ASSIGNED COMMAND (THROUGH THE CONTACT OFFICER) WILL ROUTINELY AUTHORIZE VISITS.)**

Position Description: **IN THIS PARAGRAPH INCLUDE POSITION DESCRIPTION INFORMATION SO THERE IS NO DOUBT AS TO THE DUTIES AND RESPONSIBILITIES OF THE FOREIGN OFFICIAL. BE AS COMPLETE AND AS DESCRIPTIVE AS POSSIBLE TO ENSURE A COMPLETE UNDERSTANDING BY HQDA. INCOMPLETE OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS AT HQDA, THE RETURN OF THE DDL FOR REWRITE, OR IN HQDA NONCONCURRENCE WITH THE DDL.**

5. AUTHORIZED FOR RELEASE/DISCLOSURE: IN THIS PARAGRAPH IT MUST BE CLEARLY STATED WHAT INFORMATION UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY IS/WILL BE AUTHORIZED FOR RELEASE. IT IS IMPORTANT THAT THE DDL DEVELOPING AUTHORITY BE DETAILED IN OUTLINING PORTIONS OF PROGRAMS, SYSTEMS, STUDIES, ETC. THAT THIS DDL IS DESIGNED TO COVER. THIS PARAGRAPH SHOULD PROVIDE SPECIFIC DETAILS AS TO THE BODY OF INFORMATION THAT THE INDIVIDUAL WILL REQUIRE ACCESS TO IN THE PERFORMANCE OF HIS DUTIES. TERMINOLOGY USED MUST BE CLEARLY DESCRIPTIVE OF THE INFORMATION TO BE RELEASED. THE ANTICIPATED LEVEL OF CLASSIFICATION SHOULD BE LISTED FOR EACH SPECIFIC TYPE OF INFORMATION. INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS AT HQDA AND THE RETURN OF THE DDL FOR REWRITE.

6. NOT AUTHORIZED FOR RELEASE/DISCLOSURE: THIS PARAGRAPH MUST SPECIFY THE LIMITS ON THE DISCLOSURE AUTHORITY. INCOMPLETE INFORMATION OR UNCLEAR STATEMENTS WILL RESULT IN STAFFING DELAYS AT HQDA AND/OR THE RETURN OF THE DDL FOR REWRITE. AS A MINIMUM THE FOLLOWING INFORMATION SHOULD BE INCLUDED: The following CMI is not authorized for release or disclosure under the terms of this DDL. Requests for exceptions to these restrictions must be forwarded through foreign disclosure channels to HQDA. Army.

a. GENERAL:

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

Information under the cognizance of another Military Department.

Proprietary information owned by a private firm or citizen.

Information obtained from a foreign government unless the foreign government authorizes the disclosure to a third party. The authorization must be in writing.

Data which carries any caveats or markings which limit access.

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

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

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

Low Observable Requirements or Advanced Signatures Data.

Non-Cooperative Target Recognition Data.

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

b. SPECIFIC:

SPECIFIC ITEMS LISTED AS NOT AUTHORIZED FOR RELEASE MUST BE INDICATED AT THE SAME LEVEL OF DETAIL AS IN PARA 5 ABOVE. INFORMATION THAT WAS CLASSIFIED UNDER THE ORIGINAL CLASSIFICATION AUTHORITY OF AN INDIVIDUAL/AGENCY OTHER THAN THE DELEGATION AUTHORITY SPECIFIED IN THIS DDL IS NOT AUTHORIZED FOR RELEASE WITHOUT THE WRITTEN APPROVAL OF THAT INDIVIDUAL/AGENCY. PARAGRAPH 7 PROVIDES PROCEDURES FOR DISCLOSURE OF CMI NOT UNDER THE COGNIZANCE OF THE DISCLOSURE AUTHORITY LISTED IN THIS DDL.

7. PROCEDURES: THE FOLLOWING INFORMATION (BUT NOT LIMITED TO) MUST BE INCLUDED IN THIS PARAGRAPH: The following procedures will be followed concerning the disclosure or denial of CMI authorized under the terms of this DDL.

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

b. **(APPLICABLE ONLY FOR DOCUMENTATION WHICH MAY BE REQUESTED BY AN LNO OR HIS GOVERNMENT).** Classified documents will be released to foreign **(IDENTIFY)** representatives only through government to government channels.

c. **(APPLICABLE ONLY FOR DOCUMENTATION APPROVED FOR RELEASE TO AN LNO OR HIS GOVERNMENT).** Transfer of classified documents to foreign **(IDENTIFY)**government representatives will be processed through...**(CLEARLY DEFINE APPROPRIATE FOREIGN DISCLOSURE CHANNELS I.E. THE SECURITY DIVISION, INSTALLATION SUPPORT ACTIVITY). IF THE LNO HAS BEEN AUTHORIZED BY HIS GOVERNMENT IN HIS EXTENDED VISIT REQUEST TO RECEIPT FOR CMI, ADD:** For purposes of government to government channels, **(IDENTIFY)** is authorized to receipt for CMI identified for release to his government. Documents will be forwarded directly to the foreign **(IDENTIFY)** embassy or provided to a duly authorized representative of the receiving government such as an LNO **(IDENTIFY, such as the UK LNO certified to HQ TRADOC).**

d. Records of Disclosure or Denial of Classified Military Information:

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

(a) First time disclosures based on one of the following: new information or new (higher) classification level. (See further explanation in example 1).

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

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

(2) The Security Division, Installation Support Activity **WILL** enter the disclosure into the Foreign Disclosure and Technical Information System (FORDTIS) data base.

(3) If a FORDTIS terminal is not available, the DD Form 1822, will be checked for completeness by the supporting Security Division, Installation Support Activity **(STATE WHICH ACTIVITY)** and forwarded to MACOM **(IDENTIFY)** level for entry into FORDTIS. Instructions for data entry are in DoD 5230.18M, The Foreign Disclosure and Technical Information System Users Manual.

e. Army originated CMI not classified by the command or agency designated in this DDL may be disclosed with the approval of the designated foreign disclosure authority at the MACOM **(IDENTIFY)** level. MACOM **(IDENTIFY)** level disclosure authorities will coordinate directly with appropriate MACOMs or MACOM equivalents on the disclosure of CMI to support this DDL.

f. Brief all **(IDENTIFY, such as MICOM)** personnel who will deal with **(IDENTIFY)** regarding the specific scope and terms of his/her certification.

g. CMI under the cognizance of another military department or defense agency will be forwarded through foreign disclosure channels to Headquarters, Department of the Army for coordination and adjudication.

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

a. Become familiar and ensure compliance with the duties of the contact officer and restrictions on exchange personnel as stated in AR 380-10, and the terms of this DDL.

Figure D–2. DDL for liaison officer and exchange officer—Continued

b. Brief **(IDENTIFY)** concerning DA and local policies and procedures affecting his/her status and performance of functions, as well as customs of the US Army; and render advice and assistance to ensure compliance with such policies and procedures.

c. Evaluate all requests from **(IDENTIFY)** for intra-agency and intra-MACOM consultations and visits, and assist in training activities that are consistent with the terms of this DDL.

d. Receive, evaluate and respond to--or refer to the appropriate authorities for response--all requests for information from **(IDENTIFY)** and coordinate responses with agency or MACOM foreign disclosure authorities, as necessary.

e. **FOR LNOs ONLY, STATE:** Require that all visit and information requests which are outside the terms of this DDL be submitted in accordance with applicable DA guidance through his/her military attache in Washington, DC to HQDA.

f. Notify HQDA through foreign disclosure channels anytime there is a change in contact officer or when **(IDENTIFY)** departs.

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

Appendix E
Conditions of Release Statements

E–1. As prescribed in paragraph 4-8f, appropriate statements governing the use and dissemination of DA CMI and CUI released in documentary form to foreign governments and international organizations are to be affixed to the documentary material prior to release. These statements are to be affixed as prescribed, irrespective of the presence or absence of other statements limiting dissemination or distribution prescribed by AR 70-31.

E–2. The following statement is to be affixed to all CMI and CUI released in documentary form:

> This information is furnished with the understanding that it is to be used for defense purposes only; that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States; that it is not to be revealed to another country or international organization without the written consent of the United States Government department or agency furnishing the information.

E–3. For documentary material containing CMI or CUI in Category 4 (Production Information), the following statement is to be added to that in paragraph E-2:

> The United States Government offers no objection to the use, for production purposes, of the information contained in the attached plans/specifications/technical data/other information, to the extent of the rights of the United States Government therein. However, this release of information does not in any way constitute a license to make, use, or sell the subject matter of any privately owned inventions which may be embodied or described in the information so furnished. Any manufacture, use, or sale which the recipient makes of any such inventions disclosed in the information received herein is at the risk of the recipient.

E–4. All documentary material that contains CMI or CUI which constitutes technical information (see definition in glossary) other than Category 4 information—and that is not to be authorized for use in production—is to be released "for information only" and is to bear the following statement in addition to that in paragraph E-2:

> This information is provided on the further understanding that it is to be used solely for the purpose of background information; that it accordingly is to be treated as having been provided in confidence; that the recipient is to use its best endeavors to ensure that the information provided herein is not dealt with in any manner likely to prejudice the right of any private owner thereof to obtain patent or other like statutory protection thereof; and that the recipient will obtain the express written consent of the United States government department or agency furnishing the information if it desires that the information herein be authorized for manufacture or use for other than defense purposes.

Appendix F
Sample Certification of Conditions and Responsibilities

The following is a sample format of information to be used for certification of conditions and responsibilities (see figs F-1 anf F-2).

Figure F–1. Sample certification to be signed by foreign liaison officers

(Office Symbol) *Letterhead* *(Date)*

I understand and acknowledge that I have been accepted for assignment to ***(name and location of organization to which assigned)*** in a liaison capacity as agreed between the ***(name of the country's defense establishment)*** and the United States Army. I further understand and acknowledge that I shall comply with the following conditions and responsibilities:

a. The purpose of the assignment is provide liaison between (name of the US establishment) and ***(name of the foreign establishment).*** There shall be no access to technical data or other information except that which is authorized by US authorities.

b. I understand that my activities shall be limited to the representational responsibilities of my government and will not perform duties that are reserved by law or regulation to an officer or employee of the U.S. Government.

c. Access to information shall be limited to that information determined by my contact officer to be necessary to fulfill the functions of liaison officer.

Figure F–1. Sample certification to be signed by foreign liaison officers—Continued

d. All information to which I may have access during this assignment shall be treated as information provided to my government in confidence and shall not be further released of disclosed by me to any other person, firm, organization, or government without the prior written authorization of the host government.

e. I have been briefed on, understand, and shall comply with all applicable security regulations of the host government.

(Signature)
(Typed Name)
(Grade and/or Title)
(Date)

Figure F–2. Sample certification to be signed by exchange officers

(Office Symbol) *Letterhead* *(Date)*

I understand and acknowledge that I have been accepted for assignment to *(name and location of organization to which assigned)* as agreed between the *(name of the country's defense establishment)* and the United States Department of Defense. I further understand and acknowledge that I shall comply with the following conditions and responsibilities:

a. The purpose of the assignment is to gain knowledge of the organization, management, and operation of the host defense establishment. There shall be no access to technical data or other information except that which is required to perform the duties of the position to which I am assigned.

b. I will perform only functions as described in the Position Description for my work assignment and shall not act in any other capacity for my government.

c. Access to information shall be limited to that information determined by my designated host supervisor to be necessary to fulfill the functions described in the Position Description for my work assignment.

d. All information to which I may have access during this assignment shall be treated as information provided to my government in confidence and shall not be further released or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the host government.

e. I shall not be appointed to a position that shall require me to exercise command or supervision over host government employees.

f. I have been briefed on, understand, and shall comply with all applicable security regulations of the host government.

(Signature)
(Typed Name)
(Grade and/or Title)
(Date)

Glossary

Section I
Abbreviations

ABCA
American, British, Canadian and Australian nations

AECA
Arms Export Control Act

AMC
US Army Materiel Command

AMCMI
Army Materiel Command, Office of the Deputy Chief of Staff for Intelligence

AR
Army Regulation

ARMA
US Army Military Attache

ARSTAF
Army Staff

ASA(RDA)
Assistant Secretary of the Army (Research, Development and Acquisition)

BMDO
Ballistic Missile Defense Organization

CFR
Code of Federal Regulations

CG
Commanding General

CIA
Central Intelligence Agency

CJCS
Chairman, Joint Chiefs of Staff

CMI
Classified Military Information

COCOM
Coordinating Committee for Multilateral Export Controls

COE
Chief of Engineers

COMSEC
Communications Security

CONUS
Continental United States

CUI
Controlled Unclassified Information

DA
Department of the Army

DAMI-CIS
Department of the Army Military Intelligence - Security Countermeasures Division

DAMI-CIT
Department of the Army Military Intelligence - Technology Transfer Division

DCI
Director of Central Intelligence

DCID
Director of Central Intelligence Directive

DCSINT
Deputy Chief of Staff for Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations and Plans

DDEP
Defense Development Exchange Program

DDL
Delegation of Disclosure Authority Letter (See appendix E)

DEA
Data Exchange Agreement

DIA
Defense Intelligence Agency

DIS
Defense Investigative Service

DISC4
Director of Information Systems for Command, Control, Communications and Computers

DISP
Defense Industrial Security Program

DOD
Department of Defense

DOS
Department of State

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DPEP
Defense Personnel Exchange Program

DSAA
Defense Security Assistance Agency

DTIC
Defense Technical Information Center

EAR
Export Administration Regulations

ECP
Engineering change proposal

ENDP
Exception to National Disclosure Policy

FDO
Foreign Disclosure Officer

FIS
Foreign intelligence service

FMS
Foreign Military Sales

FOIA
Freedom of Information Act

FORDTIS
Foreign Disclosure and Technical Information System

FORSCOM
US Army Forces Command

FVS
Foreign Visits System

GSOMIA
General Security of Military Information Agreement

HQ
Headquarters

HQDA
Headquarters, Department of the Army

IEP
Information exchange program

IMET
International Military Education and Training

INSCOM
US Army Intelligence and Security Command

ISM
Industrial Security Manual

ITAR
International Traffic in Arms Regulations

ITO
Invitational travel orders

JCO
Joint Certification Office

JCP
Joint Certification Program

JCS
Joint Chiefs of Staff

LNO
Foreign Liaison Officer

LOA
Letter of Offer and Acceptance

MACOM
Major Army Command

MCTL
Militarily Critical Technologies List

MOA
Memorandum of Agreement

MOU
Memorandum of Understanding

MWDDEP
Mutual Weapons Development Data Exchange Program

MWO
Modification work order

NATO
North Atlantic Treaty Organization

NDP
National Disclosure Policy

NDP-1
National Disclosure Policy

NDPC
National Disclosure Policy Committee

NIAG
NATO Industrial Advisory Group

NPLO
NATO Production and Logistics Organization

NSCID
National Security Council Intelligence Directive

NTIS
National Technical Information Service

OASA(RDA)
Office of the Assistant Secretary of the Army for Research, Development, and Acquisition

OCONUS
Outside the continental United States

ODCSINT
Office of the Deputy Chief of Staff for Intelligence

ODCSLOG
Office of the Deputy Chief of Staff for Logistics

ODCSOPS
Office of the Deputy Chief of Staff for Operations and Plans

OJCS
Office of the Joint Chiefs of Staff

OPSEC
Operations Security

OSD
Office of the Secretary of Defense

OUSD(P)
Office of the Under Secretary of Defense (Policy)

P&A
Price and availability

PCO
Procuring Contracting Officer

PEP
Personnel Exchange Program

PIP
Product improvement proposal

PM
Project Manager

POC
Point of contact

PPP
Program Protection Plan

RAC
Request for authority to conclude

RAN
Request for authority to negotiate

R&D
Research and Development

RD&A
Research, Development, and Acquisition

RDEC
Research, Development, and Engineering Center

RFI
Request for information

RFP
Request for Proposal

RSI
Rationalization, Standardization, and Interoperability

RVA
Request for visit authorization

SAO
Security Assistance Office

SCI
Sensitive Compartmented Information

SDI
Strategic Defense Initiative

SEEP
Scientist and Engineer Exchange Program

TA/CP
Technology Assessment/Control Plan

TCP
Technology Control Panel

TDY
Temporary duty

TJAG
The Judge Advocate General

TPO
Technical project officer

TRADOC
US Army Training and Doctrine Command

TSG
The Surgeon General

TTCP
The Technical Cooperation Program

US
United States

USACIDC
US Army Criminal Investigation Command

USAISC
US Army Information Systems Command

USASAC
US Army Security Assistance Command

USASSDC
US Army Space and Strategic Defense Command

USC
United States Code

Section II
Terms

ABCA Standardization Office
ABCA primary standardization office acts as the official office or record for the ABCA program. Provides continuous review of program and recommends action to expedite progress or resolve differences. Quadripartite office that integrates standard military items or programs that are eligible for member nation requisition or participation. US items and programs are consolidated by the US Army Materiel Command.

Attache
Diplomatic official or military officer attached to embassy or legation, especially in technical capacity.

Acquisition-related meeting
Meeting at which information that is to be presented describes DA activities related to the 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.

Certification
Formal recognition by DA of working relationship with representative of foreign government (such as, Liaison Officer) for specified purposes and on recurring basis over agreed period of time.

Classified Contract
Any contract that requires, or will require, access to classified information (Confidential, Secret, or Top Secret) by the contractor or its employees in the performance of the contract. Contract may be a classified contract even though contract document is not classified.

Classified Military Equipment
Military equipment that is itself classified; contains classified information that may be derived or revealed from its operation or testing; or will require the disclosure of classified information for operation, employment, maintenance, or training.

Classified Military Information
Information originated by or for DOD or its departments or agencies or under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL as described in Executive Order 12356. Classified military information may be in oral, visual, or materiel form. (Table 1 of this regulation further defines the eight categories into which classified military information has been subdivided.)

Combined Information
Military information that, by agreement, is declared to be combined by the US Government and one or more other national governments (or an international organization), irrespective of origin of information.

Conclusion/consummation (of an agreement)
Act of signing, initialing, responding to, or otherwise indicating acceptance of agreement, as negotiated.

Contact Officer
DA official designated in writing to oversee and control all contacts, requests for information, consultations, and other activities of foreign representatives who are assigned to, or are visiting, a DA activity. For PEP programs, host supervisor may be the contact officer. Contact Officer will be briefed on his duties by the FDO. All visit and requests for information received by the Contact Officer will be coordinated with the FDO.

Controlled Unclassified Information
Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of originating country. It includes US information determined to be exempt from public disclosure in accordance with AR 70-31 and AR 25-55 or subject to export controls in accordance with ITAR or EAR.

Cooperative research and development
Any method by which the United States and one or more other national governments (or an international organization) cooperate to make better use of their collective research and development resources. Cooperative research and development includes technical information exchange, harmonization of requirements, cooperative development of materiel, interdependent R&D, and agreement on standards.

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

Critical technology
Technology that consists of:

a. Arrays of design and manufacturing know-how (including technical data).

b. Keystone manufacturing, inspection, and test equipment.

c. Keystone materials.

d. Goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to military potential of any country—or combination of countries—and compromise of which may prove detrimental to US security.

Defense information/technology
Any weapons, weapon system, munitions, aircraft, vessel, boat, or other implement of war; any property, installation, commodity, materiel, equipment, supply, or goods used for the purposes of furnishing military assistance or making military sales; any machinery, facilities, tool, materiel, supply, or other item necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any other defense articles; or any component or part of the preceding articles--less merchant vessels and articles governed by the Atomic Energy Act of 1954, as amended.

Defense service
Any service, test, inspection, repair, training, publication, or technical or other assistance, or defense information used for the purpose of furnishing security assistance-less design and construction services.

Delegation of Disclosure Authority Letter (DDL)
Letter issued by the appropriate designated disclosure authority describing classification levels, categories, scope, and limitations about information that may be disclosed to specific foreign governments or foreign representatives for a specified purpose. ODCSINT, DA (DAMI-CIT) will review and approve all delegation of disclosure authority letters.

Designated Disclosure Authority
Official delegated disclosure authority in accordance with AR 380-10, to control disclosures of CMI and CUI at DA subordinate commands or staff elements.

Disclosure
Conveying of CMI or CUI, through oral or visual means to an authorized representative of a foreign government.

Document/documentary materiel
Any recorded information, regardless of its medium, physical form, or characteristics.

Extended visit authorization
See Visit authorization.

Facility clearance
Often referred to as Reciprocal Facility Security Clearance. An administrative determination that the facility is eligible, from a security viewpoint, for access to classified information of the same or lower security category as the level of clearance being granted. Facility clearances will not be granted to contractor activities located outside the United States, Puerto Rico, or a US possession or trust territory.

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

Foreign Disclosure and Technical Information System (FORDTIS)
Automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release CMI and to deny CUI to foreign governments.

Foreign exchange personnel
Military or civilian officials of foreign governments assigned to DA activities under PEP agreements and perform duties prescribed by a position description, for the DA activity.

Foreign ownership, control, or influence (FOCI)
Situation in which a foreign national, firm, or government is assumed to possess dominance of or authority over a US firm to such a degree that the foreign entity may gain unauthorized access to US CMI.

Foreign representative
Either a foreign national or a representative of a foreign interest.

Functional agreement
An agreement not formally deemed to be an international agreement, including--

a. A contract made under the Defense Acquisition Regulation.

b. A foreign military sales credit agreement.

c. A foreign military sales Letter of Offer and Acceptanced.

d. A foreign military sales letter of intent executed on DD Form 2012 (US DOD Letter of Intent).

e. A NATO Standardization Agreement or ABCA Quadripartite Standardization Agreement that records the adoption of (1) like or similar military equipment, ammunition, supplies, or stores, or (2) operational, logistic, or administrative procedures.

f. A lease or loan under section 61 of the Arms Export Control Act or under the Foreign Assistance Act of 1961, chapter 2, part II.

g. An agreement that establishes only administrative procedures.

Government-to-government channels
Principle that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed on by the governments involved. In either case, information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.

Information
Knowledge in a communicable form.

In-house meeting
A meeting attended exclusively by military personnel or civilian employees of DOD (may be expanded to include DOD contractor personnel, but only if the meeting is related exclusively to matters involving a specific contract already let).

Intelligence
Information and related materiel describing US 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 US foreign intelligence collection efforts. May or may not include SCI.

International activities and projects
DA actions and initiatives formally accomplished under auspices both of various international agreements-bilateral and multilateral-and functional agreements, as defined in AR 550-51. Selected examples are MOUs promoting RSI among NATO and ABCA member nations and MOUs providing for cooperative R&D, including co-development, dual production, MWDDEPs, DDEPs, and security assistance programs.

International agreement
a. An agreement, but not a functional agreement, that is concluded with one or more foreign governments (including their agencies, instrumentalities, or political subdivisions) or with an international organization and--(1) Is signed or agreed to by one of the following: (a) civilian or military officers, (b) employees of any DOD organizational element, or (c) representatives of the Department of State or other agencies of the US Government. (2) Signifies the intention of the parties to be bound in international law. (3) Is identified as one of the following: international agreement, Memorandum of Understanding, exchange of notes, exchange of letters, technical arrangement, protocol, note verbale, aide memoire, agreed minute, plan, contract, arrangement, or some other name having similar legal consequence.

b. Any oral agreement that meets the criteria in a above, Such an agreement must be reduced to writing by the DOD representative who enters into the agreement.

c. A NATO Standardization Agreement that provides for either of the following: (1) mutual support or cross-servicing of military equipment, ammunition, supplies, and stores, or (2) mutual rendering of defense services, including training.

International Organization
Entity established by recognized governments pursuant to international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

International Traffic in Arms Regulations (ITAR)
Department of State implementation of section 38 of the Arms Export Control Act. ITAR governs export of information and materiel that are defense-related and listed on the US Munitions List.

Joint information
Military information over which two or more DOD, or two or more Federal departments or agencies, exercise control, jurisdiction, or security awareness.

Liaison officers
Foreign government officials, either military or civilian employees, certified by their governments to act as representatives of that government to a DA element in connection with bilateral or multinational programs or projects.

Meeting
Any conference, seminar, symposium, exhibit, convention, training course, or other gathering during which CMI or CUI is disseminated.

Military information
Classified or unclassified information under control and jurisdiction of DOD or its components, or of primary interest to them. (May be embodied in equipment or may be in written, oral, visual, or other communicable form.)

Munitions list
Listing of articles designated as arms, ammunition, and implements of war and are subject to licensing requirements imposed by Arms Export Control Act through ITAR.

National Disclosure Policy (NDP-1)
NDP-1 promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance required by US departments and agencies having occasion to release CMI to foreign governments and international organizations. In addition, it establishes and provides for management of interagency mechanism and procedures required for effective implementation of the policy. This policy is based on NSDM 119, 'Disclosure of Classified United States Military Information to Foreign Governments and International Organizations,' 20 July 1971, as reaffirmed and augmented by White House Memorandum of the same subject, date 6 June 1978.

National Disclosure Policy Committee (NDPC)
Central authority for formulation, promulgation, administration, and monitoring of the NDP-1. Consists of general and special members and their alternates. General members have a broad interest in all aspects of committee operations. Special members have a significant interest in some, but not all, aspects of committee operations.

a. General Members will serve as representatives of the Secretaries of State, Defense, Army, Navy, and Air Force; and the Chairman, Joint Chiefs of Staff.

b. Special Members will serve as representatives of the Secretary of Energy; Director of Central Intelligence; Under Secretary of Defense for Policy; Under Secretary of Defense for Acquisition; Assistant Secretary of Defense for Command, Control, Communications and Intelligence; Assistant to Secretary of Defense (Atomic Energy); Director, Defense Intelligence Agency and Director, Strategic Defense Initiative Organization.

One-time visit authorization
See Visit authorization

Originating DA component
DA activity that exercises original classification jurisdiction for CMI or CUI.

Proprietary Information
Information, e.g., trade secrets, owned by a private individual or other entity.

Rationalization, Standardization, and Interoperability (RSI)
Means of increasing coalition warfare capabilities of US, allied, and friendly nation forces through use of common (standard) or

interoperable procedures and resources. Applicable to concepts, doctrine, tactics, logistics, procedures, training, and materiel and non-materiel requirements, and is essential to successful integration of allied forces during conduct of combined operations.

Recurring visit authorization
See Visit authorization

Release
Conveying of CMI or CUI, through oral or visual disclosure or actual physical transfer, to an authorized representative of a foreign government. Routine technology transfer decisions Decisions made to approve or deny disclosure of Army controlled technology that are consistent with guidelines established by higher authority. Also, decisions made to approve or deny public disclosure or selective release of unclassified technical data based on guidance in the MCTL and AR 70-31.

Security assistance
Group of programs authorized by Foreign Assistance Act of 1961, as amended, and Arms Export Control Act, as amended, and Arms Export Control Act, as amended, or other related statutes by which the US Government 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
Written confirmation, requested by and exchanged between governments, of security clearance level or eligibility for clearance of their national contractors and citizens. Includes statement by responsible official of a foreign government or international organization that original recipients of US CMI possesses requisite security clearance and are approved by their governments for access to information of security classification involved on behalf of the government or organization and that recipient government will comply with security requirements specified by the United States.

Security manager
DA official designated to be responsible for supervising all security aspects of a classified meeting.

Sponsorship
a. In context of meeting, provision of DA resources (such as, personnel and funds) in support of the meeting.
b. In context of visit by foreign visitor to US industry, DA authorization for disclosure of information on US Munitions List by a US commercial firm, irrespective of whether the firm possesses a munitions license (that is, sponsorship of an exemption to the ITAR).
c. In context of visit by foreign representative, statement rendered by foreign government or international organization on behalf of foreign representative indicating that the latter's interaction with DA is officially sanctioned by the former, which assumes full responsibility for visitor's actions and for information that may be disclosed to visitor. (Also known as "security assurance".)

Strategic war plan
Plan for overall conduct of war.

Technical data package
Technical description of item or service adequate for use in procurement. Description will be sufficiently complete to control configuration to required degree of design disclosure and item quality to required level. Package will consist of all applicable technical data, such as plans, drawings, and associated lists, specifications, purchase descriptions, standards, models, performance requirements, quality assurance provisions, and packing data.

Technical information/data
Knowledge including scientific knowledge that is in communicable form and relates to research, development, engineering, testing, evaluation, production, operation, use and maintenance of munitions (arms, ammunition, and implements of war), and other military supplies and equipment.

Training
Formal or informal instruction of foreign nationals in the United States or overseas by one of the following:
a. Officer or employees of the United States, contract technicians, or contractors (including instruction at civilian institutions).
b. Correspondence courses, technical, educational, or information publications and media of all kinds, training aids, orientation, training exercises, and military advice to foreign military units and forces (including their military and civilian personnel).

Visit authorization
There are three type of visit authorizations, as outlined below.
a. One-time visit authorization permits contact by foreign representative with DA element or DA contractor facility for single short-term occasion (normally less than 30 days) for a specified purpose.
b. Recurring visit authorization permits intermittent visits by foreign representatives to DA element or DA contractor facility over specified period of time for government-approved license, contract, or agreement, or other program when information to be released has been defined and approved for release in advance by US Government.
c. Extended visit authorization permits single visit by foreign national for extended period of time. Extended visit authorizations are to be used when foreign national is required to be in continuous contact with DA element or DA contractor facility beyond 30 days, for one of the following situations:
(1) Foreign government contract or joint program (such as, joint venture, representative to a joint or multinational program, and so forth).
(2) Participation in exchange program under PEP or SEEP.
(3) Training, except for individuals on Invitational Travel Orders.
(4) Liaison officers certified to DA element.

Section III
Special Abbreviations and Terms

This section contains no entries

Index

Army Materiel Command (AMC), 1-5d(1), 1-11, 2-8c(1), 2-8f(2)(b),2-11b(3), 2-11c(2), 4-7a, 5-30b, 5-34a, Appendix C

Assistant Secretary of the Army (Research, Development and Acquisition, 1-9, 1-12b, 2-8f(2)(b), 2-11b(2), 2-11c(1), 3-4d(1), 3-6b(6), 3-9, Appendix C

Chief of Engineers, 1-13, 2-8f(2)(b)

Classified military information,
disclosure authorities, 2-11
disclosure conditions, 2-5
disclosure criteria, 2-4a
disclosure limitations, 2-6

Classified military information, 1-18, 1-19, Glossary

Conferences
planning for foreign attendance, 6-7
procedures, 6-8
types, 6-2 thru 6-6

Contact officer, 5-6
during visits, 5-6a
for exchange personnel, 5-6c
for liaison officers, 5-6b

Controlled unclassified information, 1-18,
disclosure authority, 2-10

DA Foreign Disclosure Program,
during hostilities, 4-7c
international activities, 3-1, 3-2, 3-8
licensed commercial basis, 3-5
objectives, 1-4b
security assistance-related, 3-3, 3-4, 3-7

DA Technology Security Program,
DCSINT direction, 1-5d
objectives, 1-4a
policy, 2-8

Delegation of disclosure authority letter, 3-1a, 5-4, Appendix E

Deputy Chief of Staff for Intelligence,
responsibilities, 1-5

Deputy Chief of Staff for Logistics,
responsibilities, 1-7

Deputy Chief of Staff for Operations and Plans,
responsibilities, 1-8

Designated disclosure channels, 1-20

Diplomatic status, 5-2

Director, Information Systems for Command, Control, Communications and Computers,
responsibilities, 1-13

DoD International Technology Transfer Panel, 1-5b(2)

Eighth US Army, 1-16

Exchange personnel, 5-30
access to electronic mail, 5-38, 5-39
administering, 5-35
processing nominations for, 5-34
restrictions, 5-31, 5-32
supervisors responsibilities, 5-37

False impressions, 2-2, 2-7b, 4-8

FORDTIS, 4-10, 5-9

Foreign disclosure security classification guidance, 1-22, Table 3

Foreign test and evaluation, 3-6

International Visits Program,
ABCA, 5-22
Canadian visits, 5-23
delegation of authority, 5-25
disclosure during, 4-2
evaluation and processing, 5-17
NATO, 5-20
purpose, 5-8
requests for visit authorization, 5-16
standards of appearance, 5-5
US-sponsored visits, 5-13
visits to contractor facilities, 5-17

Liaison officers,
access to electronic mail, 5-38, 5-40
disclosure, 4-4, 5-29b
establishment of LNO positions, 5-27
general restrictions, 5-26
misconduct, 5-29e
processing requests, 5-28
services provided, 5-29a
visits, 5-29c

National Disclosure Policy Committee, 1-5b(1)

National Disclosure Policy,
disclosure levels, 2-3a
exceptions, 2-3b

Personnel Exchange Program,
disclosure, 3-11, 4-3
proponent,

Program Protection Plan, 2-8e(3)

Security protection and assurances, 1-21

Technology Assessment/Control Plan,
responsibility for, 2-8e(2)

Technology Control Panel, 2-8f

The Judge Advocate General,
responsibilities, 1-12

The Surgeon General, responsibilities, 1-12

US Army Criminal Investigation Command, 1-15

US Army Europe, 1-16

US Army Intelligence and Security Command, responsibilities, 1-10

US Army Pacific, 1-16

US Army Southern Command, 1-16

US/Canada Joint Certification Program,
certified contractors, 4-6
release of CUI, 4-6a, 4-6b

*U.S. G.P.O.:1995-387-857:80427