

Department of the Army  
Headquarters, USAFCEFS  
455 McNair Avenue, Suite 100  
Fort Sill, OK 73503  
01 March 11

USAFCEFS Regulation 380-10

Security & Intelligence Division  
DPTMS

**PROCEDURES FOR FOREIGN VISITORS AND FOREIGN PERSONNEL  
ASSIGNED TO U.S. ARMY FIRES CENTER OF EXCELLENCE  
AND FORT SILL**

---

**Summary.** This policy establishes responsibilities, and administrative procedures governing security requirements and functional responsibilities for administering visits by foreign representatives and/or foreign forces at US Army Fires Center of Excellence and Fort Sill (USAFCEFS).

**Applicability.** This policy applies to all USAFCEFS activities located on Fort Sill.

**Supplementation.** Supplementation of this regulation is prohibited without prior approval from the Chief of the Security & Intelligence Division, DPTMS, 1651 Randolph Road, Fort Sill, OK 73503.

**Suggested Improvements.** The proponent of this regulation is the Security & Intelligence Division, DPTMS. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms).

**Distribution.** This regulation is distributed solely through the DHR, ASD Homepage at [http://sil-www.army.mil/dhr/Admin\\_Svcs/Index.html](http://sil-www.army.mil/dhr/Admin_Svcs/Index.html).

---

**Table of Contents**

	<b>Paragraph</b>	<b>Page</b>
<b>Chapter I. Introduction</b>		
1-1. Purpose	1-1	3
1-2. References	1-2	3
1-3. Explanation of Abbreviations and Terms	1-3	3
<b>Chapter II. Responsibilities</b>		
2-1. Commanding General, USAFCEFS	2-1	3
2-2. Chief of Staff, USAFCEFS	2-2	3
2-3. Public Affairs Officer (PAO)	2-3	3
2-4. Protocol, USAFCEFS	2-4	4
2-5. USAFCEFS Foreign Disclosure Officer (FDO)	2-5	4
2-6. Foreign Disclosure Representative (FDR)	2-6	5

**USAFCoEFS Regulation 380-10, 01 March 11**

2-7. Contact Officer (CO)	2-7	5
2-8. USAFCoEFS Personnel	2-8	8
<b>Chapter III. Disclosure of Information to Foreign Representatives</b>		
3-1. General	3-1	8
3-2. Foreign Embassy Requests	3-2	9
3-3. FLO and PEP Requests for Information (RFI)	3-3	9
3-4. Processing RFIs	3-4	9
<b>Chapter IV. International Visits Program</b>		
4-1. Requests for Visit Authorization (RVA)	4-1	11
4-2. Types of Visits	4-2	11
4-3. Procedures for Processing a Visit Request	4-3	12
4-4. Amendments to RVA	4-4	13
4-5. Foreign Visitor Responsibilities	4-5	13
4-6. Foreign Visitor Misconduct	4-6	14
4-7. Informal Coordination	4-6	15
4-8. Visits by Formal Invitation	4-7	15
4-8. Visit Decision Types	4-8	15
<b>Chapter V. Foreign Liaison Officer (FLO) Program</b>		
5-1. Purpose of the U.S. Army FLO Program	5-1	16
5-2. Definition of Terms and Roles of FLOs	5-2	16
5-3. Types of Liaison Officers (LOs)	5-3	16
5-4. Program Exchange Personnel (PEP)	5-4	18
5-5. Access to USAFCoEFS Facilities	5-5	19
<b>Chapter VI. Information Disclosure for Doctrine &amp; Training</b>		
6-1. Information Disclosure for Doctrine	6-1	20
6-2. Information Disclosure for Training	6-2	20
<b>FIGURES</b>		
Figure 1. Foreign Embassy Request for Information		24
Figure 2. Foreign Liaison Officer and Personnel Exchange Program Officer; Simple Requests for Information		25
Figure 3. Foreign Liaison Officer and Personnel Exchange Program Officer; Multiple Simple Requests for Information		25
Figure 4. Foreign Visit Request Process		26
<b>ANNEXES</b>		
ANNEX A. POLICY AND MILITARY CONSIDERATIONS		27
ANNEX B. INFORMATION ASSURANCE		29
ANNEX C. TIPS		33
ANNEX D. REPORTING PROCEDURES		35
<b>APPENDIXES</b>		
APPENDIX A. REFERENCES		36
APPENDIX B. GLOSSARY		37
Abbreviations		37

Terms		38
-------	--	----

**Chapter I  
Introduction**

**1-1. Purpose.** This regulation establishes policies and procedures to protect the security of U.S. Army Fires Center of Excellence & Fort Sill (USAFCoEFS) missions, organizations, and personnel; and establishes within the USAFCoEFS a policy to provide security requirements and functional responsibilities for administering information exchange and visits by foreign representatives and/or foreign military assigned to USAFCoEFS.

a. Foreign Disclosure with allied and other friendly countries is an increasingly important and complex part of our national security and defense acquisition strategy. An open exchange of information, technology and Tactics, Techniques and Procedures (TTPs) is needed to succeed on the battlefield.

b. It is imperative that proposed disclosures reflect the need for striking a proper balance between pursuit of our mutual defense and foreign policy directives on the one hand and the preservation of the security of our military “secrets” or “protected” unclassified information on the other. This must be measured on a case-by-case basis consistent with US national security objectives and the complex inter-workings of our National Disclosure Policy (NDP-1).

c. Foreign Disclosure should always result in a clearly defined benefit for the US and is limited to information necessary for the purpose for which disclosure is made.

**1-2. References.** Required and related publications are listed in Appendix A.

**1-3. Explanation of Abbreviations and Terms.** Abbreviations and terms used in this Regulation is explained in the glossary (Appendix B).

**Chapter II  
Responsibilities**

**2-1. Commanding General, USAFCoEFS.** The Commanding General will appoint in writing a Foreign Disclosure Officer (FDO) and authorize the FDO to disclose Controlled Unclassified Information (CUI) for which USAFCoEFS is the originator/proponent to foreign representatives.

**2-2. Chief of Staff, USAFCoEFS** is responsible for approval of documentary disclosures, on a case-by-case basis.

**2-3. Public Affairs Officer (PAO)** is responsible for certifying information as “PUBLIC DOMAIN.” An item’s appearance on the Internet (particularly a non-DoD website) does not, by itself, certify that the military information is officially “public domain.”

## USAFCoEFS Regulation 380-10, 01 March 11

**2-4. Protocol, USAFCoEFS,** on request, assist in arranging for quarters or transportation; however, it must be made clear to visitors or their military attaches that all expenses concerning the visit, including quarters, transportation, and subsistence, are the responsibility of the visitors. As visits are occasionally canceled with little or no notice, Site Visit Contact Officers (SVCOs) should refrain from making commercial reservations for services on behalf of foreign visitors. Instead, assistance should be limited to recommending and providing telephone numbers for commercial services to foreign visitors or their military attaches.

**2-5. USAFCoEFS Foreign Disclosure Officer (FDO)** is responsible for:

a. The oversight and controlling of specific disclosures of Classified Military Information (CMI) to non-US entities.

b. Coordinating requests for foreign visit authorization and disclosure of information to foreign nationals.

c. Certification of foreign nationals assigned to the USAFCoEFS; i.e. (Foreign Liaison Officers (FLO), Personnel Exchange Program (PEP) Officers, Country Liaison Officers (CLO) and Security Assistance Liaison Officers (SALO).

d. Ensuring the requirements of the Department of Defense (DoD) /Army/Training and Doctrine Command (TRADOC) Foreign Disclosure Programs are implemented.

e. Administrative staffing of requests for CMI or CUI. Since the majority of official foreign government and international organization requests for US information are submitted through foreign disclosure channels, the FDO will facilitate the administrative processing of all Requests for Information (RFI) that are forwarded by a higher HQ, another Command, through foreign disclosure channels, or through unsolicited correspondence that may eventually involve the disclosure of CMI or CUI.

f. Establishing a foreign disclosure education and oversight program within the USAFCoEFS.

(1) The DoD Foreign Disclosure course for Contact Officers is available online: [dss.mil](http://dss.mil). Go to the Enrol page, set up an account and then go to the FDO course. The course consists of five courselets which are designed to educate in the international security environment and provide familiarization with international programs and activities that involve disclosure.

(2) The TRADOC Foreign Disclosure Overview course is available on line at: <https://tradocapps.monroe.army.mil/dcsintrng>.

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

## USAFCoEFS Regulation 380-10, 01 March 11

h. Forward a copy of training certification for FLO/PEP Contact Officers to HQ TRADOC (ATIN-SD).

### **2-6. Foreign Disclosure Representative (FDR) will:**

a. Be appointed in writing.

b. Advise and assist the FDO with the processing and coordination of foreign government Request for Visit Authorizations (RVA) and/or foreign representative requests for CMI and CUI within their assigned staff, FD ratings for training courses, and any other matters pertaining to disclosure of CUI or CMI to foreign government representatives or the public.

c. Be a DoD civilian or US military member who has knowledge of their organization's mission and OPSEC requirements (preferably a GS11/SFC).

d. Be trained and certified and receive an annual refresher briefing; therefore, the nominated FDR should have 12 months retain ability. The FDR is not a release authority. CMI and CUI will only be released after review/coordination with the FDO.

e. Act as the principal advisor for FD issues to the organization commander or director.

**2-7. Contact Officer (CO).** There are two types of COs at Fort Sill; those required to support short term visits (Site Visit Contact Officers) and those required for established FLOs, PEPs and CLOs (Contact Officers). The Contact Officer is the primary point of entry for all USAFCoEFS RFI from foreign personnel.

a. Site Visit Contact Officers (SVCO) will:

(1) Be designated in writing to facilitate and oversee activities of foreign visitors for a specific visit request to the USAFCoEFS. The identification of the SVCO for an approved one-time visit request satisfies the requirement for the contact officer to be named in writing.

(2) Be available to the foreign officials during the entire visit.

(3) Become familiar with AR 380-10, local supplementation and reportable foreign visitor activity under provisions of AR 381-12, Threat Awareness and Reporting Program (TARP).

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

## USAFCoEFS Regulation 380-10, 01 March 11

(5) Coordinate with and obtain guidance from the following Fires Center of Excellence (FCoE) personnel:

(a) FDO/FDR: for information concerning the preparation of briefings or discussion items in oral or visual form. The SVCO must avoid creating a "false impression" pertaining to the release of government information. Visitor requests for discussions outside the approved purpose of the RVA will be denied, with a recommendation to direct the request to the foreign visitor's military attaché for action.

(b) Security manager or operations security (OPSEC) officer for information concerning agency or command activities occurring simultaneously with the foreign visit and from which visitors may need to be excluded. Escorts are required when the visitors cannot otherwise be denied access to information or operations outside the scope of the approved visit.

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

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

(7) Maintain a log of all request for information and information provided. Upon completion of visit, provide log to the FDO.

(8) At the direction of the Commanding General, ensure that foreign visitors are aware of and comply with foreign disclosure and security requirements regarding the visit.

(9) Notify the 902d Military Intelligence (MI) office of any foreign visitor activity that is reportable under the provisions of AR 381-12.

(10) In the event of any misconduct on the part of a foreign visitor during the visit, provide a written report to ODCS G-2 through command channels.

b. Foreign Liaison/PEP Contact Officer will:

(1) Be designated in writing by the commander.

(2) Will be equivalent or higher rank/grade to FLO/PEP.

(3) Will be physically accessible to and have daily contact with the FLO/PEP.

(4) Will become familiar with the provisions of AR 380-10 and the FLO/PEP's official certification. The CO will assist the FDO in ensuring the certification is current and updated as needed.

## USAFCoEFS Regulation 380-10, 01 March 11

(5) Will complete the online Foreign Disclosure course for Contact Officers within 30 days of appointment and provide a copy to the FDO.

(6) Will be identified in FLO's certification letter (primary & alternate).

(7) Will receive an annual briefing from the FDO.

(8) Will initially brief the FLO/PEP on Headquarters Department of the Army (HQDA) and local policies and procedures affecting his status and performance of duties as well as customs of the U.S. Army, and render advice and assistance to ensure compliance with such policies and procedures. This will include a briefing informing the FLO/PEP that foreign nationals cannot purchase US Uniforms from a US Government Source.

(9) Will ensure the FLO/PEP understands his/her duties of assigned position and have the FLO/PEP sign a certification statement form; provide a copy to the FLO/PEP and FDO.

(10) In conjunction with the FDO/FDR, evaluate all requests from the FLO/PEP for consultations and visits and assist in arranging activities that the contact officer deems substantively consistent within the terms of the certification. Consultations and visits beyond the terms of the certification require the submission of formal visit requests by the parent foreign government embassy in Washington, D.C.

(11) Receive, evaluate and recommend/refer all requests involving CMI outside the scope of the USAFCoEFS to the FDO.

(12) Receive, evaluate and refer all requests involving non-releasable CUI to the FDO for administrative processing and forwarding to the originator/proponent.

(13) The CO will notify the FDO when the designated contact officer/alternate is changed or upon permanent departure of the foreign representative under his or her oversight.

(14) Will notify the supporting counterintelligence and local security offices of any foreign visitor activity, which is reportable under the provisions of AR 381-12.

(15) Will comply with the procedures regarding misconduct according to AR 380-10.

(16) Will maintain a log of all request for information and information provided and provide a log to the FDO at the beginning of each quarter.

(17) Will appoint a sponsor for each foreign national with an approved extended visit request. The sponsor will contact the visitor at least 2 months prior to their arrival. The sponsor will be responsible for greeting and all in processing activities.

## 2-8. USAFCoEFS Personnel.

a. During new employee orientation sessions, receive initial briefing from FDO/FDR regarding AR 380-10, local supplementation and reportable foreign visitor activity under provisions of AR 381-12, Threat Awareness and Reporting Program (TARP).

b. Complete the TRADOC Foreign Disclosure Overview course and provide the certificate to their organization security manager. The TRADOC Foreign Disclosure Overview Course is a mandatory requirement for all military and civilian personnel assigned to the USAFCoEFS.

c. Receive an annual Foreign Disclosure refresher briefing. Annual refresher training is a mandatory requirement for all military and civilian personnel assigned to the USAFCoEFS.

d. Respond to requests for information in a timely manner. Permission to release any information will be given in writing and approved by the organization's FDR. Information provided will be comprehensive and easy to understand by uninformed personnel. If information cannot be released to foreign nations, a detailed justification is mandatory.

## Chapter III.

### Disclosure of Information to Foreign Representatives

**3-1. General.** US personnel are responsible for ensuring information provided to foreign representatives meets all regulatory guidelines. The FDO's approval is not required to provide military information that has been officially approved for public release or information that is unclassified and not controlled/caveated to a foreign government or international organization. The FDR is authorized to release unclassified open-source material. All other information will be reviewed by the FDO prior to release. The two methods for releasing of CMI or CUI will be oral and visual; an exception to allow the disclosure in documentary form (to include notes taken during briefings or discussions) may be made, provided that the visit request security assurance specifically states the individual may assume custody on behalf of the foreign government and the proponent or his or her designee approves the request. In all cases, the provisions of AR 380-5 and DOD 5220.22-M shall apply.

a. Basic criteria for disclosure:

- (1) Access: Is foreign access in the best interest of the U.S. (need-to-know)?
- (2) Protection: Can foreign entity provide equivalent security protection as U.S.?

## USAFCoEFS Regulation 380-10, 01 March 11

(3) Government-to-Government: Is disclosure or transfers of information or technical data for official government-to-government use?

b. Prohibited disclosure; unless appropriate approval is obtained:

(1) Information obtained from a foreign government.

(2) Information obtained from Coalition forces.

(3) Information obtained from other Services.

(4) Information originated by or for another department or agency.

**3-2. Foreign Embassy Requests (Figure 1):** Other nations may submit requests for information through their military attaché attached to their embassy. These requests will be submitted to OSD and follow the chain of command through HQDA and TRADOC to the FDO. These requests are normally received from the TRADOC FDO or through TRADOC Army Capabilities Integration Center (ARCIC) and should include the following information:

a. The requesting country, subject and classification (if known) of information to be disclosed, and originator of the information (if known).

b. The purpose of disclosure (i.e., foreign military sales program, subject matter expert information exchange, etc.).

c. Requested release date.

**3-3. FLO and PEP Requests for Information (RFI):** RFIs from the FLOs and PEPs assigned to USAFCoEFS will be submitted in writing to the appointed CO (primary or alternate).

a. The CO is responsible for coordinating with the FLO/PEP to define the scope of the request and obtain details of information requested. If the request falls within the scope of the LNO/PEP's certification and need-to-know (NTK), the CO will coordinate with the appropriate organization within the USAFCoEFS for release. The CO will ensure the organization's FDR has reviewed and approved release of the information prior to providing it to the FLO/PEP.

b. Requests for information outside the scope of the certification or for which the originator is outside of the USAFCoEFS will be forwarded to the FDO for release IAW Army and TRADOC procedures and policy. The FDO will coordinate with the originator to obtain and gain approval to release the information requested. The FDO will prepare notification for the CO who will provide the final response to the requesting FLO or PEP.

**3-4. Processing RFIs (Figures 2-3).**

## USAFCoEFS Regulation 380-10, 01 March 11

a. General. To ensure programmatic, policy, operational, technology and security-related issues are evaluated, the CO will coordinate with the FDO prior to the release of any information.

(1) If the RFI is a simple request, the CO will coordinate directly with the appropriate organization's FDR to obtain the information.

(2) If the RFI is complicated and involves multiple organizations, the CO will draft an OPORD for publication by G3. The OPORD will task organization FDRs having responsibility for the information to provide the requested information to the CO.

(3) If information must be obtained from another Command or agency, the CO will forward the request to the FDO for action.

b. Processing CMI requests:

(1) All releases for Classified Military Information must be processed through the FDO.

(2) All requests must be officially requested in writing by the foreign embassy/entity; verbal requests will not be accepted. FLOs and PEPs will submit requests for CMI through their CO.

(3) All releases are government-to-government and must be justified by an international agreement, Memorandum of Understanding (MOU), or accepted letter of offer.

(4) Release will require the written approval of both the Original Classification Authority (OCA) and the designated disclosure authority for the CMI in question.

c. Processing Controlled Unclassified Information requests:

(1) All requests must be officially requested in writing by the foreign embassy/entity; verbal requests will not be accepted. FLOs/PEPs will submit requests for CUI through their Contact Officer.

(2) Originator/proponent, in coordination with the organization's FDR can approve release of CUI.

d. Approving Requests to Disclose Information.

(1) FDRs will obtain assistance from the FDO when receiving requests directly from foreign governments, international organizations, or from US personnel asking for information for a foreign entity/government (i.e., training materials, mobile training teams, setting up schools / training facilities in a foreign country, etc.).

## USAFCoEFS Regulation 380-10, 01 March 11

(2) The FDO will forward requests through disclosure channels to other TRADOC FDOs for materials in which they retain original classification authority (OCA) or proponentcy.

(3) The FDO will follow proper security protocols and forward requests through disclosure channels to the HQ TRADOC FDO for MACOM-to-MACOM assistance.

NOTE: AR 380-10 prohibits the FLOs or PEPs from directly contacting US personnel for release of information and further ensures the Contact Officer or the FDO releases the information/data to the FLO or PEP.

### **Chapter IV. International Visits Program**

#### **4-1. Requests for Visit Authorization (RVA).**

a. All RVAs must be submitted through the requesting country's embassy to the Office of the Deputy Chief of Staff (ODCS) G-2, Foreign Disclosure Branch via Foreign Visit System (FVS). ODCS G-2 will forward the request to TRADOC, who in turn, forwards the visit request to USAFCoEFS FDO. USAFCoEFS FDO will determine the appropriate POC for the visit and ensure Protocol and other interested parties are kept informed through the Information Exchange Working Group. The POC will reply to FDO regarding the RVA acceptance NLT the suspense listed on the RVA. Unannounced or unscheduled visits to DA facilities where foreign representatives arrive at an Army activity or facility without official approval will not be permitted to proceed. In those instances, the Army command or agency shall immediately report the incident to ODCS, G-2, which will provide instructions to the Army command or agency and notify the parent government's military attaché of the violation.

b. Visitors who are general/flag officers or civilian equivalent rank/grade must include biographical data on the RVA. This includes biographic information concerning visitors of general officer rank and civilians holding equivalent government appointments. This assists in the proper staffing of the RVA with Protocol.

#### **4-2. Types of Visits.**

a. One-Time Visit. Contact by foreign representatives with a DoD component or DoD contractor facility for a single short term occasion (normally fewer than 30 days) for a specified purpose.

b. Recurring Visit. Intermittent, recurring visits by foreign representatives with a DoD component or DoD contractor facility over a specified period of time for a government approved license, contract, agreement or other program when the

## USAFCoEFS Regulation 380-10, 01 March 11

information to be released has been defined and approved for release in advance by the U.S. Government, subject to annual review and revalidation.

c. **Extended Visit.** A single visit by a foreign representative located in the U.S. for a duration that exceeds 30 days. Extended visit authorizations are to be used when a foreign representative is required to be located at or in continuous contact with a DoD component or contractor facility beyond 30 days, for one of the following situations:

(1) A foreign government contract, joint program, agreement, or license.

(2) Certification as a PEP participant, FLO or Standardization Representative (STANREP).

d. **Emergency Visits.** Defined as a visit request submitted within seven calendar days of the proposed visit. The request must state a specific government approved contract, international agreement, or announced request for proposal. The request must fully explain and justify the reason for the late submission. The requestor must alert the Regional Desk Officer of the emergency visit by phone or email. Emergency visits are only approved as a single, one-time visit, and cannot be amended.

### **4-3. Procedures for Processing a Visit Request (Figure 4).**

a. To submit a one-time or recurring visit request:

(1) Request should be submitted through FVS in sufficient time for it to arrive at the installation to be visited at least **30** days prior to visit.

(2) The request must contain complete and accurate information concerning the nature, purpose, locations and duration of the visits, as well as identification data regarding the visitor(s).

b. To submit an extended visit request:

(1) Request should be submitted through FVS in sufficient time for it to arrive at the installation to be visited at least **90** days prior to visit.

(2) RVA contains complete and accurate information concerning the nature, purpose, locations and duration of the visits, as well as identification data regarding the visitor(s). If dependents are to accompany the visitor specifically FLOs and PEP participants, the request must also identify the dependent for DEERS purposes.

c. Each year the Office of the Deputy Under Secretary of Defense, Policy Support (Foreign Visits System) sends a letter informing embassy personnel of a holiday moratorium. RVAs submitted for visit dates during the moratorium timeframe will be returned without action unless the visit is to attend a previously scheduled conference, meeting, or is mission essential. The moratorium is necessary, because DoD activities

## USAFCoEFS Regulation 380-10, 01 March 11

traditionally operate at reduced levels during the Christmas holiday period. Visits submitted during the holiday moratorium for visits to occur after the moratorium period will be accepted for processing.

### 4-4. Amendments to RVA.

a. All modifications to approved visits will be proposed by amendments submitted through the FVS for consideration.

b. Prior to submitting the proposed amendment through the FVS, the attaché must contact the designated Contact Officer at USAFCoEFS. Once the CO concurs with the proposed modifications to the approved RVA, the attaché must ensure an amendment is submitted through the FVS. The amendment submission should reference the concurrence of the CO.

c. Amendments may only be submitted for the following:

(1) Add or delete names of visitors (additions require identifying data).

(2) Change originally proposed date(s).

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

### 4-5. Foreign Visitor Responsibilities.

a. Foreign visitors must contact the SVCO specified on the approved RVA at the organization or facility to be visited at least 72 hours (excluding Saturdays, Sundays, and holidays) in advance of each visit. Recurring visitors must contact the SVCO three weeks in advance of proposed visit.

b. All military visitors must wear the appropriate military attire of the respective country unless otherwise directed.

c. Visitors must have, in their possession, personal identification that depicts a photograph, an identification number, date of birth, and nationality. Passports are generally recommended as the form of identification that meets the criteria.

d. Visitors may not arrive at USAFCoEFS until the visit request for the visitor is approved.

e. Visitors must be prepared to pay all expenses associated with the entire visit (i.e., travel, lodging, meals, etc.).

f. Visitors must provide (and the embassy must ensure that the RVA contains), complete and accurate information concerning the nature, purpose, locations and duration of the visits, as well as identification data regarding the visitor(s).

## USAFCoEFS Regulation 380-10, 01 March 11

g. The visitor(s) must have adequate English language capability or, if necessary, arrange to bring an interpreter.

h. All foreign visitors with an approved extended visit request will comply with the Fort Sill policies regarding on-post housing.

(1) Accompanied personnel will be offered on-post housing equivalent to their grade/rank and number of dependents in the U.S. military. All personnel are subject to waiting list procedures due to availability of appropriate housing.

(2) Single/Unaccompanied personnel will not be offered on-post quarters due to lack of Bachelor Officer Quarters on post. The Housing Services Office and sponsor will provide assistance in locating off-post housing.

(3) For foreign personnel whose parent country provides furnishings for their quarters, the host nation will be solely responsible for any maintenance, repairs or storage costs associated with those furnishings.

**4-6. Foreign Visitor Misconduct.** For the purpose of this regulation, misconduct or alleged misconduct on the part of foreign visitors is categorized as either personal misconduct or official misconduct. This distinction is necessary in order to facilitate appropriate reporting actions by DA personnel.

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

b. **Official Misconduct.** Events or actions seen as inappropriate or improper that are related to the purpose of the visitors presence at a U.S. Army activity, command, organization, or DoD contractor facility. Official misconduct refers to the misuse, abuse of, or violations of permissions, authorities, access, and procedural guidelines governed in Terms of Certification, Delegation of Disclosure Authority Letters, and/or Requests for Visit Authorizations.

c. The following instances will be reported IAW the provisions of AR 381-12 with an information copy to ODCS, G-2. In the instance when the foreign visitor:

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

## USAFCoEFS Regulation 380-10, 01 March 11

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

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

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

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

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

d. All other instances of official misconduct or alleged misconduct will be reported to ODCS, G-2.

**4-7. Informal Coordination.** Foreign representatives are permitted to contact DA offices or staff elements for informal coordination of administrative details only. This coordination does not eliminate the need for an RVA. The proposals and requests become official only upon the submission of an RVA to ODCS G-2, Foreign Disclosure Branch.

**4-8. Visits by Formal Invitation.** On occasion, DoD officials invite foreign representatives to visit U.S. Army facilities and installations to attend meetings or conferences. When foreign visitors are invited to travel to Army facilities or installations on Invitational Travel Orders (ITO) or honorariums published by a competent authority, these visits do not require a foreign visit request. However, for the purpose of responding to an invitation, the embassy must use the visit request format to provide and validate to the sponsoring Army organization the names and personal identification information of the visitors, including security clearances. If the inviting Army organization elects not to issue ITO or honorariums to the visitors, the embassy must provide an RVA, and if possible, a copy of the invitation.

**4-9. Visit Decision Types.** After receipt of a complete RVA that meets all administrative processing requirements, the USAFCoEFS FDO will coordinate the visit and then provide the embassy one of the following responses:

a. Approval: Approval indicates that the visit is part of a valid government-to-government program, project or agreement under the auspices of the DoD. The recommendation for approval must include the name and commercial duty telephone number of the Contact Officer who will host and coordinate the visit. Sponsor for extended visit foreign visitors will also be identified in the recommendation for approval.

## USAFCoEFS Regulation 380-10, 01 March 11

b. Deny: If USAFCoEFS determines that it is unable to host a visit request or that the information associated with the request cannot be authorized for disclosure, USAFCoEFS must submit a recommendation for denial of the visit request. Such a recommendation must include the rationale for the decision as well as any special instructions or comments to the embassy (e.g., request for resubmission of visit request at a later date, etc.).

c. Return without action: Visits are returned without action when an RVA does not meet the minimum administrative processing requirements; does not contain all the necessary information and/or the request could not be coordinated appropriately within DoD. RVA that are returned without action may be corrected by the embassy and resubmitted for reconsideration.

d. Cancel: Upon the request of the Embassy.

### **Chapter V. Foreign Liaison Officer (FLO) Program**

**5-1. Purpose of the U.S. Army FLO Program.** The Army Foreign Liaison Officer Program was established to facilitate cooperation and mutual understanding between the U.S. Army and the armies of allied and friendly nations.

#### **5-2. Definition of Terms and Roles of FLOs.**

a. A FLO is a foreign government military member or civilian employee who is authorized by his or her government and is certified by a DA command or agency in connection with programs, projects or agreements of interest to the governments. FLOs are expected to present the views of their parent government regarding issues of mutual interests, namely those that may be raised by the DA command or agency to which they are certified.

b. Upon arrival to their organization, all FLOs will be assigned a sponsor and receive a briefing from their contact officer on DA and local policies & procedures, duties of assigned position and will sign a certification statement form stating such. A copy will be provided to the FLO and FDO.

#### **5-3. Types of Liaison Officers (LOs).**

a. Operational FLOs: An operational FLO is a foreign government representative who is assigned to a DA command or agency pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education. Thus a country-specific liaison officer agreement between the U.S. Army and each foreign army participating in the FLO program, such as a FLO MOA or FLO MOU, is a prerequisite for establishment of operational FLO positions.

## USAFCoEFS Regulation 380-10, 01 March 11

(1) Reciprocity is not a requirement of the FLO program (i.e., there is no requirement for a one-to-one exchange of FLOs between the U.S. and the foreign government).

(2) FLOs are not to be used as a member of the Army's work force.

(3) FLOs may participate in the activities of the organization to which assigned when the assignment is in support of a specific international program, project or agreement. Such participation must be described in the certification letter and job description.

(4) FLOs may only have access to that information, classified or unclassified, that has been authorized for release to their government as described in the job description.

(5) FLOs may assume custody of documentary information for transfer to their government only when they are authorized in writing by their government to receive such information.

(6) Administrative support to FLOs (Admin FLO). Occasionally, a FLO requires administrative support personnel to assist him/her with the duties assigned by his/her government. In such instances, the FLO's government, via an accredited military attaché, may submit a request to establish an administrative position in support of a FLO. However, administrative support personnel are not authorized to request or receive information from DA commands or activities. Admin FLOs are not authorized to act on behalf of the supported FLO or to represent the foreign government.

b. Security Assistance FLOs (SALO): A foreign government representative who is assigned to a DA element or contractor facility pursuant to a requirement that is described in a Letter of Acceptance (LOA). Thus, an LOA is a prerequisite for the establishment of SALO positions.

c. Country Liaison Officers (CLO): This type of FLO includes foreign representatives who are assigned to U.S. Army commands or activities under ITOs to perform specific administrative oversight functions regarding students of their respective governments. They are not to act as FLOs. There will not be an exchange of information between our country and theirs. These allied personnel will only have access to the same information their students have under their FMS case. CLOs will be assigned to the International Student Division (ISD).

(1) Duties will consist of:

(a) Assisting with the administrative details for International Military Students (IMS) and their country.

## USAFCoEFS Regulation 380-10, 01 March 11

(b) Being the contact between the International Student Division (ISD) and the IMS.

(c) Assisting in the orientation, to include in- and out-processing of IMS.

(d) Assisting in correcting problems associated with dress, personal appearance, grooming standards, and IMS indebtedness.

(e) Being responsible for whatever action is necessary in connection with breaches of discipline, to include honor code violations, involving IMS.

(f) Assisting in routine inspections of IMS and their quarters.

(g) Assisting in administrative details regarding the disposition of IMS.

(h) Advising the IMSD of any national holidays, customs, and traditions that should be recognized.

(i) Making routine administrative reports as required by their government.

(j) Pay IMS any allowances received from the home country if so directed by his/her government.

(k) The CLOs will have the same access to medical and dental care as the IMS, and the same requirements for medical coverage.

(l) The CLOs are subject to the same security restrictions as those governing IMS.

### **5-4. Program Exchange Personnel (PEP).**

a. The PEP program is a program under which military and civilian personnel of the Department of the Army and military and civilian personnel of the defense ministries and/or military services of foreign governments, pursuant to the terms of an international agreement, occupy positions with and perform functions for a host organization to promote greater understanding, standardization, and interoperability.

b. Upon arrival to their organization, all PEPs will be assigned a sponsor and receive a briefing from their contact officer on DA and local policies & procedures, duties of assigned position and will sign a certification statement form stating such. A copy will be provided to the PEP and FDO.

c. PEPs are assigned to positions within and perform functions for the organization to which they are assigned. They do not represent their government as is the case of FLOs. However, they are still foreign nationals.

## USAFCoEFS Regulation 380-10, 01 March 11

d. Procedures must be developed to preclude the PEP's inadvertent or unauthorized access to CMI and CUI that has not been authorized for release to their country. PEPs will not be assigned to positions that would give them access to information not authorized for release to their government.

e. PEPs will not be used for training, nor combined with, or as a substitute for, the functions of a FLO.

f. PEPs will not be used as a conduit for exchanging technical data or other controlled information between governments.

g. PEPs will not be given any security responsibilities (e.g., escort duties, document custodian, security checks, etc.).

h. PEPs will not have permanent custody of CMI or CUI. They may have supervised access to material authorized for disclosure during normal duty hours at the place of assignment. They may not have unsupervised access to libraries or document catalogs unless the information contained therein is releasable to the public.

i. PEPs will not have access to restricted areas or to the following types of information:

(1) RESTRICTED DATA or FORMERLY RESTRICTED DATA.

(2) Information systems security information unless there is a current agreement with the PEP's government that permits access.

(3) CMI or CUI provided by another government, unless access approved, in writing, by the originating government.

(4) Compartmented Information, unless authorized by a current agreement with the participant's government.

(5) Information bearing a special handling notice that restricts access, except when authorized by the originator, in writing.

**5-5. Access to USAFCoEFS Facilities.** Foreign nationals, including PEPs and FLOs, may not have uncontrolled access to USAFCoEFS facilities. They may, however, have unescorted access when all of the following conditions are met:

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

b. Access is required for official purposes on a frequent basis (i.e., more than once a week).

## USAFCoEFS Regulation 380-10, 01 March 11

c. In a restricted facility, a badge or pass will be issued to identify the bearer as a foreign representative and is valid for the specific facility during normal duty hours.

### **Chapter VI Information Disclosure for Doctrine and Training**

#### **6-1. Information Disclosure for Doctrine.**

a. Determining appropriate caveats for doctrinal publications is not a foreign disclosure (FD) issue. However, all doctrine writers (i.e., military personnel, federal civil servants, and civilian contractors) must ensure they know their data sources and list them appropriately. Further, they need to know if the information they've obtained from a caveated source is releasable to non-US government personnel. This can be accomplished by identifying data sources during development of the doctrinal publication, marking their drafts appropriately (recommend paragraph by paragraph similar to marking a classified document), and maintaining an audit trail of all source data (i.e., page, paragraph, document title/number, date of documents, etc.). This will facilitate the release determination of USAFCoEFS-generated doctrinal material to foreign entities (i.e., FLOs, PEPs, students, Embassy requests, etc.).

b. Before revising previously applied restrictive caveats to USAFCoEFS - generated publications, doctrine personnel must ensure the data is releasable to non-US government personnel. If a referenced caveated publication is not USAFCoEFS - originated, the Command "owning" the publication must be queried for release if USAFCoEFS is using information from "their" publication. They must also be informed of our intent in the usage of their information (i.e., release to FLO, placed in training that includes foreign students, etc.). This can be accomplished by the FDR (with assistance from the FDO, if required).

**6-2. Information Disclosure for Training.** It is the policy of the U.S. to avoid creating false impressions of its willingness to make available classified military material, technology, or information. Therefore initial planning with foreign governments concerning training which might involve the eventual disclosure of classified information may be conducted only if it is explicitly understood and acknowledged that no U.S. commitment to furnish classified information or material is intended or implied until disclosure has been approved. U.S. Army personnel involved in training of foreign personnel will refrain from any commitment to furnish specific CMI or CUI until disclosure has been approved by designated disclosure authorities.

a. Minimum essential requirement: All course materials and training products containing CMI or CUI must show appropriate classification and FD restriction statements. Ensure all existing and new training courses, products, and literature have disclosure adjudication and application of appropriate restriction statement prior to release of training to foreign nationals. *Note:* Restriction statements are in addition to the distribution statements on Armywide Doctrinal and Training Literature Program (ADTLP) products.

## USAFCoEFS Regulation 380-10, 01 March 11

b. To help protect against non-approved disclosure of CMI or CUI information in training courses, materials, and products, training developers must:

(1) Maintain an audit trail of all source data (i.e., page, document title/number, date of document). This can be accomplished by identifying data sources during development of the material publication, marking their drafts appropriately (recommend paragraph by paragraph similar to marking a classified document), and maintaining an audit trail of all source data (i.e., page, paragraph, material title/number, date of material, etc.). This will facilitate the release determination of USAFCoEFS-generated material to foreign entities (i.e., FLOs, PEPs, students, Embassy requests, etc.).

(2) Forward all training course design documents (i.e., training support packages [TSPs], Programs of Instruction [POIs], and lesson plans) and training products to the FDO/FDR for determination of the appropriate category classification and the appropriate restriction statement.

(3) Apply overall and page classification markings IAW AR 380-5; apply appropriate FD restriction statements.

c. The applicable FD restriction statement (including number) should appear (as shown below) on the cover of every Training/TATS Course TSP which contains CMI or CUI and is used for training any foreign student.

FD1. The materials contained in this course have been reviewed by the course developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. This course is releasable to students from all requesting foreign countries without restrictions.

FD2. The materials contained in this course have been reviewed by the course developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. This course is releasable to military students from foreign countries on a case-by-case basis. Foreign countries desiring to place students in this course must meet one or more of the following criteria: (1) Own (a specific piece of equipment); (2) Have a signed Letter of Intent (LOI); (3) Have a waiver from HQDA; (4) Have USG release for training; (5) etc.

FD3. The materials contained in this course have been reviewed by the course developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. This course is *NOT* releasable to students from foreign countries.

FD4. The materials contained in this course have been reviewed by the course developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. Some component(s) of this course is(are) *NOT* releasable to students from foreign countries. See each Training/TATS Course TSP subcomponent/product for applicable FD restriction statement.

## USAFCoEFS Regulation 380-10, 01 March 11

d. One of the following FD numbers and restriction statements should appear on the cover of any TSP subcomponent (e.g., lesson plan, Program of Instruction, course management materials, etc.); stand-alone training products; and training literature containing CUI or CMI information. These restriction statements are in addition to the distribution statements on ADTLP publications.

FD5. This product/publication has been reviewed by the product developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. This product is releasable to students from all requesting foreign countries without restrictions.

FD6. This product/publication has been reviewed by the product developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. This product is releasable to students from foreign countries on a case-by-case basis.

FD7. This product/publication has been reviewed by the product developers in coordination with the Fort Sill Security & Intelligence Division, DPTMS foreign disclosure authority. This product is *NOT* releasable to students from foreign countries.

e. If CMI/CUI in the training product was originated by another TRADOC activity, the release must be coordinated by the USAFCoEFS FDO with the other TRADOC FDO through disclosure channels.

f. If CMI/CUI in the training product was originated outside TRADOC, the release must be coordinated MACOM to MACOM. The USAFCoEFS FDO will coordinate release with the TRADOC FDO located in the TRADOC ODCSINT.

g. All course materials and training products containing CMI or CUI must show appropriate classification and FD restriction statements (See Chap I-1-4, TRADOC Reg 350-70.)

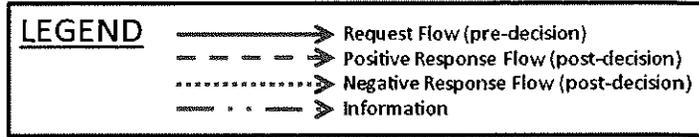
h. Course developers will refer all training materials/products containing CMI/CUI and being considered for foreign disclosure to the FDO for approval, denial, or further coordination.

i. Course developers will ensure all existing and new training courses, products, and literature have disclosure adjudication and application of appropriate restriction statement prior to release of training to foreign nationals. Coordinate with USAFCoEFS FDO and apply the appropriate classification marking and FD restriction statement (including FD number).

**USAFCoEFS Regulation 380-10, 01 March 11**

j. Commandants and trainers will ensure foreign students have access only to releasable training materials for the courses they are attending. This restriction extends to automated training databases and products.

FIGURES.



**Foreign Embassy Request for Information**

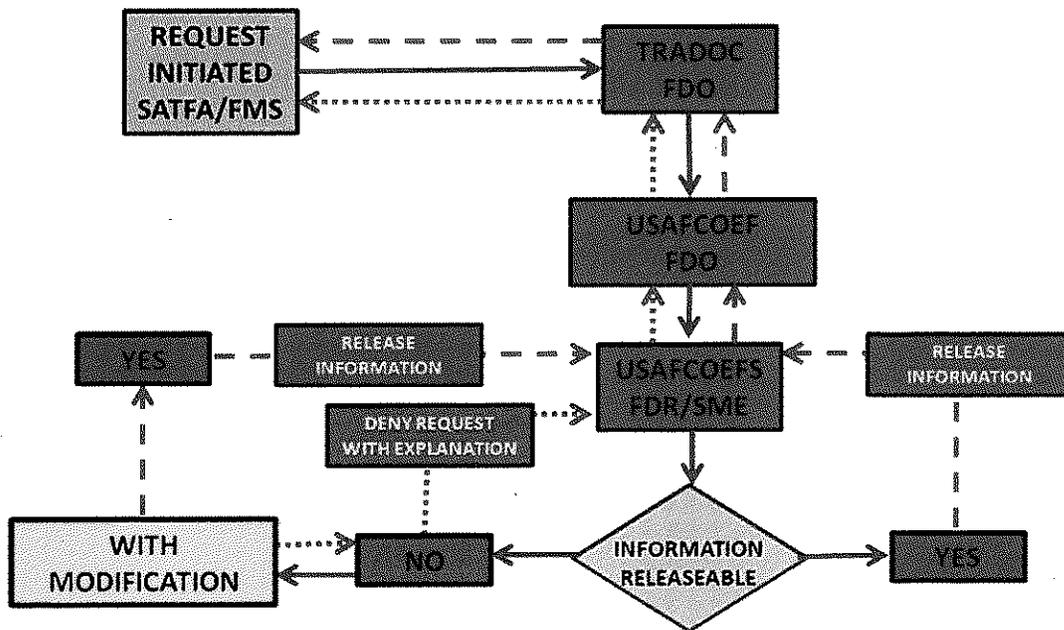


FIGURE 1

**Foreign Liaison Officer/Personnel Exchange Program Officer**  
**Simple Request for Information**

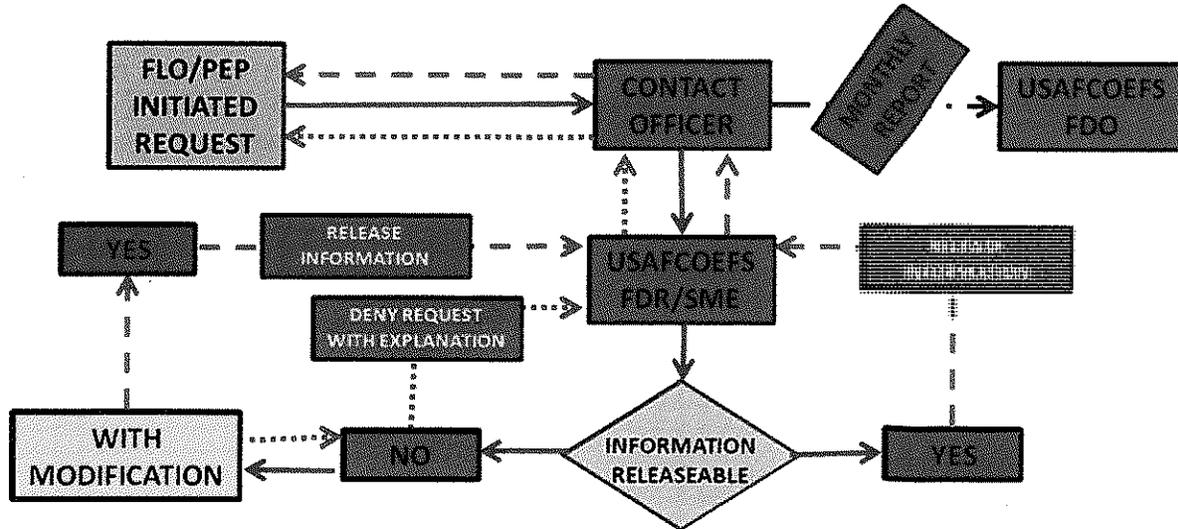


FIGURE 2

**Foreign Liaison Officer/Personnel Exchange Program Officer Multiple Requests for Information**

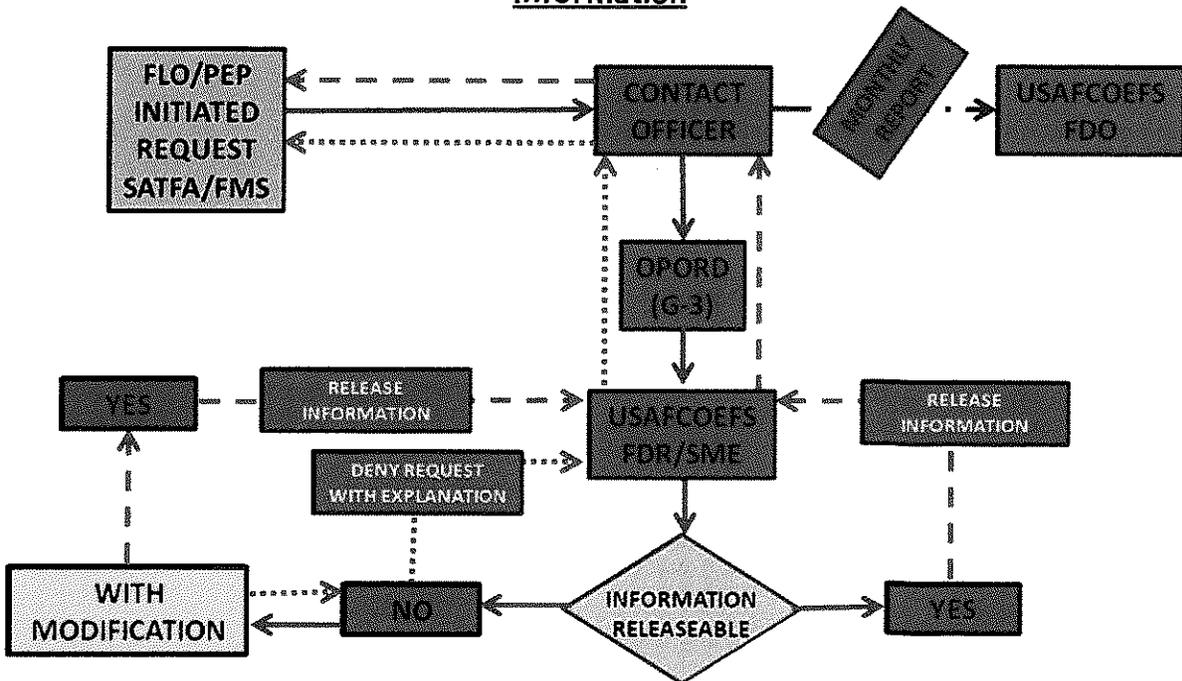


FIGURE 3

Foreign Visit Request Process

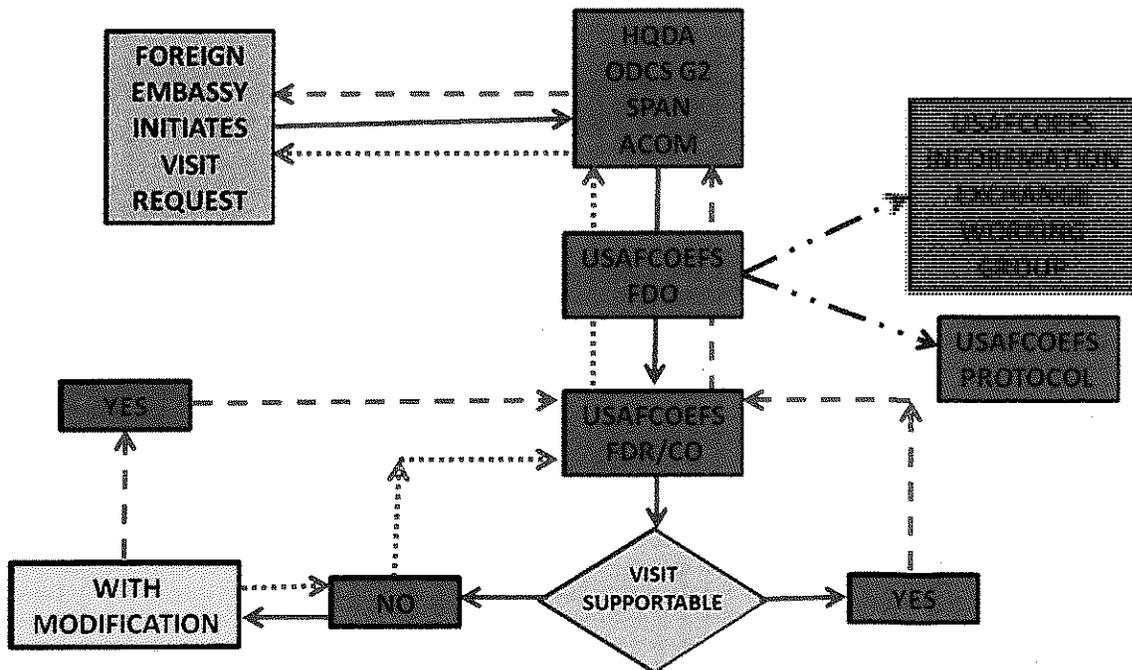


FIGURE 4

**ANNEX A  
POLICY AND MILITARY CONSIDERATIONS**

The originator or proponent of the CUI should consider the following military and political considerations in rendering a disclosure decision:

**A-1. Military Considerations.**

- Country's ability and willingness to protect sensitive US information.
- 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 precedent exists for disclosure of this particular technology or system? Are comparable systems (foreign and domestic) using the same technology already in the marketplace?
- Can the critical technology resident in the system be reverse engineered? If so, what level of effort (in terms of time, funding and manpower) is required based on the technological capability of the foreign recipient?
- Is the technology or information resident in one US Army weapons program been leveraged from another US Army weapons program? If so, has the original US Army weapons Program Manager (PM) reviewed and rendered a recommendation on the munitions license request? The technology or information may not be listed as Critical Program Information (CPI) for one program, but identified as CIP for another program.
- Are there any special considerations involved with the disclosure that requires coordination external to the US Army? For example, communications security, low observable, crypto logical information, etc. If so, have proper approvals been obtained?
- The degree of participation in collective security by the US.
- How the disclosure would affect coalition warfare in support of US policy.
- How the disclosure would increase the recipient country's offensive or defense capability.
- How the disclosure would increase the capability of friendly regional forces to provide regional security to assist the US in the protection of strategic line of communication.
- How the disclosure shall strengthen US or allied power projection.
- To what extent the disclosure is in consonance with US military plans, (e.g., the CINC Theater Engagement Plan (TEP), Army International Activities Plan (AIAP), and Army Science and Technology Master Plan (ASTMP)).
- How the disclosure would strengthen the Army Technology Base via quid pro quo resulting from this release.
- Whether or not the disclosure is consistent with Army regional Rationalization, Standardization and Interoperability policy.
- Whether or not the information supports a force structure requirement.
- Can the country's technology base support the information?
- To what degree the disclosure counters the country's threat.

**A-2. Policy Considerations.**

- The potential foreign recipient's support for US foreign policy and political objectives.
- The potential of the disclosure to deny or reduce an influence or presence in the country that is hostile to US interests.
- The effects of the regional and global strategic balance if the disclosure is approved.
- Whether or not the country has a defense treaty or political agreement with the US.
- The political benefits that could accrue to the US.
- Whether or not the disclosure assists the US in obtaining or securing base, transit, and overflight rights or access to strategic locations.
- Other countries to which the US has disclosed the information.
- The possible reaction of other countries in the region to the proposed disclosure.
- Whether or not the US is the first supplier of the information.
- The possibility that the information could fall into the hands of terrorists.
- The impact of the disclosure on the country's economy.
- Whether or not the disclosure establishes an unfavorable political precedent.
- Does the disclosure support US Foreign policy objectives?
- Before authorizing CUI disclosures, the CUI Disclosure Authority shall ensure that the contract or agreement contains the requisite access, use, and distribution clauses required before disclosing CUI to another government, international organization, or foreign contractor. CUI Disclosure Authorities may obtain assistance from the local legal office.
- If technical CUI originated by another command or agency is resident in a technical CUI document proposed for disclosure to a foreign government, the proponent command or agency of the technical CUI document is responsible for obtaining the approvals for the disclosure of that CUI data belonging to the other originator. At a minimum, Disclosure Officials should apply the principals of disclosure (i.e., disclosure criteria) to all disclosures of CUI. These specific criteria are:
  - The release must support US foreign policy, national security objectives, and military security objectives regarding the intended recipient government or international organization.
  - The release must not jeopardize US military security.
  - The disclosure must result in a clearly defined benefit to the US.
  - The proposed recipient has the intent and the capability to provide the same degree of protection as given the information by the US.
  - The disclosure is limited to that information necessary to satisfy the purpose for which the disclosure is made.

**UNAUTHORIZED DISCLOSURES OF TECHNICAL CUI DATA CONTROLLED BY  
THE ARMS EXPORT CONTROL ACT CAN RESULT IN CRIMINAL PROSECUTION**

## **ANNEX B INFORMATION ASSURANCE**

Security violations can and do occur under all circumstances. Violations are classified as deliberate or inadvertent compromises. In most cases, a violation occurs because one or more of the procedures in AR 380-5 were not followed due to lack of attention to detail or lack of knowledge.

### **B-1. Foreign Disclosure Basics**

- Access to CMI and CUI depends on the security clearance granted by the FLOs / PEOs / foreign representative's government, need-to-know, and disclosure guidance issued by the Contact Officer's servicing FDO.
- PEPs shall not have personal custody of CMI or CUI.
- FLOs may have custody of CMI as stipulated in the authorizing agreement that establishes their position and is subject to the following conditions:
- FLOs may assume custody of documentary information and act as couriers when authorized in writing by their government. US security personnel exercise oversight over the storage container. This oversight is similar to that executed by US security personnel over US storage containers. NOTE: FLOs do not have access to a classified container. The FLO's government is required to provide all necessary courier credentials.

**B-2. Automated Systems.** Authority to connect to the SIPRNet, NIPRNet or other networks by foreign nationals does not equate to authority to disclose data or access systems located on that network.

a. NIPRNet. To ensure standardized and appropriate access to the Unclassified but Sensitive Internet Protocol Routing Network (NIPRNET) by foreign officials, Information Assurance (IA) personnel will meet the requirements delineated below. Provide each authorized foreign official a .mil address on the unclassified network required for executing his or her foreign official duties as outlined in his or her respective certification. For each authorized foreign official, the local area network administrator will place a caveat or marker on the user account and all outgoing e-mails from that person identifying them as a foreign official from a specific country. In doing so, the local area network administrator will spell out the words "Foreign Official" and the country name of the foreign official and will not use an acronym for that country. In addition, the local area administrator will indicate the type of foreign official access that is granted. The required tags for each of the five categories of foreign officials would thus read as shown below (replace each hypothetical country name with the appropriate one).

(1) Foreign Liaison Officer (FLO): "Last Name, First Name Middle Initial-Foreign National-Germany-FLO." (Note: Local area network administrators will designate FLOs representing the United Kingdom, Canada, or Australia as STANREPs rather than as FLOs.)

## USAFCoEFS Regulation 380-10, 01 March 11

(2) Cooperative Program Personnel (CPP): "Last Name, First Name Middle Initial-Foreign National-Turkey-CPP".

(3) Engineer and Scientist Exchange Program (ESEP): "Last Name, First Name Middle Initial-Foreign National Israel-ESEP".

(4) Standardization Representative (STANREP): "Last Name, First Name Middle Initial-Foreign National-United Kingdom-STANREP".

(5) Military Personnel Exchange Program (MPEP): "Last Name, First Name Middle Initial-Foreign National-Italy-MPEP".

b. Limit access to foreign officials, exchange personnel, or representatives to computers that incorporate Army-mandated access and auditing controls. Approval to access the NIPRNET does not equate as authority to exchange data or access systems located on that network. The appropriate system IASO will approve access to foreign officials on an as needed basis. Similarly, the designated release or disclosure authority will grant access to the information on ISs to foreign officials on an as-needed basis.

c. E-mail signature blocks will be automatically generated for all foreign personnel, and include the foreign individual's nationality and position.

d. Full AKO accounts are authorized for AS, CA and UK FLOs/PEPs only. All others will be issued AKO email only.

e. International Military Students (IMS) who have been vetted and approved for U.S. Army training and Professional Military Education (PME) attending resident training or enrolled in the Army Distance Education Program (DEP) at U.S. Army and Army-managed schools/training activities will agree to comply with all U.S. MILDEP requirements. They are required to sign an AUP user agreement. There is no requirement for background investigations as described since in-country U.S. officials perform a security screening of each student before selection approval. To prevent inadvertent disclosure of information, international military students will be identified as students in their email address, display name and automated signature block (for example, john.i.smith.uk.stu@xxx.army.mil).

f. NIPRNET access policy and procedures for FNs in official positions as identified above, are as follows:

(1) Components or organizations will maintain records on access including the following information—

(a) Specific mission requirements for foreign access or connection.

(b) Justification for each individual FN.

## USAFCoEFS Regulation 380-10, 01 March 11

(2) Confirmation that the minimum-security requirements of this section are enacted, including the user agreement discussed below.

g. Before authorizing FN access to a specific IS on the NIPRNET, Army components will—

- (1) Ensure the information is properly processed for disclosure.
- (2) Ensure IASOs and data owners concur with the access.
- (3) Ensure the C&A documentation for the system is updated to reflect FN access.
- (4) Ensure security measures employed adhere to this policy.
- (5) Validate the identity of each FN authorized access to ISs to ensure accountability of all actions taken by the foreign user.
- (6) Ensure the FN follows appropriate security policies and procedures and that the IASO possesses the authority to enforce these policies and procedures. Before accessing any system, an FN will sign an AUP agreement that includes—
  - (a) Acknowledgment of appropriate information security policies, procedures, and responsibilities.
  - (b) The consequences of not adhering to security procedures and responsibilities.
  - (c) Identification requirements when dealing with others through oral, written, and electronic communications, such as e-mail.
  - (d) Department of the Army employees or contractors who are FNs and are direct or indirect hires, currently appointed in IA positions, may continue in these positions provided they satisfy the provisions of paragraph 4–14, DODD 8500.1, DODI 8500.2, and DOD 5200.2–R; are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the IASO and captured in the C&A package.
  - (e) FNs assigned into IT positions will be subject to the same (or equivalent) vetting as U.S. citizens.

h. FNs may hold or be authorized access to IT–II and IT–III positions provided the required background investigation has been completed or favorably adjudicated.

i. Additionally, an FN may be assigned to an IT–I position only after the IASO who owns the system and the data owner who owns the information sign a waiver and

the assignment has been approved by the CIO/G-6. The approvals will become part of the C&A package. Sign and place the waiver in the individual's security file before requesting the required background investigation. The required background investigation must be completed and favorably adjudicated before authorizing IT-I access to DA systems/networks.

j. Do not assign FNs to IT-I, IT-II, or IT-III positions on an interim basis before a favorable adjudication of the required personnel security investigation.

**B-3. Foreign Access to Secure Internet Protocol Router Network (SIPRNet).**

Consistent with current DoD policy, specific criteria has been established for foreign access to classified Defense networks; otherwise known as "SIPRNet Rel." These security requirements parallel those requirements for access to classified information for US personnel. They are as follows:

- a. Must be United Kingdom/Australian/Canadian (UK/AUS/CAN) citizen.
- b. Government personnel assigned or working in collaboration with the US Government.
- c. Hold the appropriate UK/AUS/CAN security clearance to match the level of classification and access and have a need-to-know.
- d. Willing and able to afford the CMI protection from classified disclosure.
- e. Be advised that CMI shall not be further disseminated.

**B-4. Additional Requirements.** Foreign users will be required to complete standard Information Assurance (IA) training required of any US user and then complete the "Supplementary Training for UK/AUS/CAN Personnel on SIPRNet" signature sheet. The user must also complete/sign a country-specific Non-Disclosure Agreement (NDA) acknowledging his or her responsibility as a SIPRNet user. Additionally, a modified DD Form 2875, or SAAR, must be completed. All documentation in relation to this effort will be stored with the Contact Officer and FDO. See *REL DMZ SIPRNet Policy Letter under separate cover*.

**B-5. MONTHLY REPORT.** A monthly report will be provided by the FDO to the NEC, ensuring the NEC has correctly identified all foreign officers and to enable the disable/deletion of an account once a foreign officer has departed.

**ANNEX C  
TIPS**

Contact the USAFCoEFS FDO for assistance when planning interaction with foreign nationals for any of the following circumstances:

**C-1. Visits by Foreign Nationals or Representatives of Foreign Governments.**

When you are aware that a foreign representative may wish to visit your office for government business, contact the FDO for guidance. There are several types of foreign visits, each with a different procedure and lead time. Official visits must be submitted in accordance with AR 380-10. Submissions should be received by HQDA G2 at least 30 days prior to the day of the visit.

**C-2. Presentation of Briefings or Papers to a Foreign Audience.** Technical papers or briefings (including drawings) that will be presented at a conference or meeting which could be attended by foreign nationals must first be reviewed by the FDO. If the paper is being given to a foreign audience according to a specific government-to-government agreement, such as Memorandum of Understanding (MOU) or Data Exchange Agreement (DEA), it must be provided to the FDO for review and approval before the conference or travel begins.

**C-3. Foreign Nationals Working on Government Contracts.** If a contractor submits a letter requesting a foreign national be allowed to work on a government contract, the Project Officer must evaluate the technical information involved and make a recommendation to the FDO. The FDO will conduct a disclosure review and provide a recommendation to the Contracting Officer. If the request is approved, the foreign national must be escorted at all times while on a government facility.

**C-4. Technical Meetings.** If your office is planning to host or co-host a technical meeting or conference which could include foreign nationals, you must contact the FDO at the beginning of planning for the meeting.

**C-5. Receipt of Foreign Correspondence.** If you receive correspondence from a foreign national who requests a copy of an article or a technical report or any type of official military information, forward the request and a copy of the article to the FDO. Articles that have been cleared for public release may be provided. However, you are not obligated to honor such a request.

**C-6. CMI and CUI.** CMI and CUI are treated as national security assets that must be protected and shared with foreign representatives **only** when there is a clearly defined advantage to the United States. The unauthorized disclosure of CMI and CUI can lead to the compromise of US military capabilities and underlying technologies. Likewise, military operational plans and intelligence operations and sources may be compromised. Penalties for the unauthorized disclosure of CMI and/or CUI range from administrative sanctions to criminal charges with possible fines or imprisonment.

## USAFCoEFS Regulation 380-10, 01 March 11

### **For Foreign personnel to receive CMI, they must meet these qualifications:**

a. Disclosure must be consistent with US foreign policy and security objectives. (Information cannot be used in a manner that is harmful to US personnel, interests or missions. All disclosures must have a clearly defined advantage for the US.

b. Recipient must ensure protection of CMI commensurate with that provided by the US. (Foreign personnel must treat the US CMI with the same care as US personnel treat it, such as using safes and not disseminating beyond those to whom it is authorized.)

c. Foreign personnel must have the equivalent security clearance for CMI received. (Example: If a foreign officer receives US SECRET information that is releasable to his/her country, then he/she must possess the equivalent of a US SECRET clearance.)

d. Foreign personnel have a need-to-know. (Need-to-know trumps all of the above. You provide to foreign personnel only what they have a need-to-know. Example: If a foreign officer is eligible to receive TOP SECRET information and has a TOP SECRET clearance, but requires only SECRET information to fulfill his/her mission, then he/she receives only SECRET information.)

**ANNEX D  
REPORTING PROCEDURES**

**D-1. Reporting Security Infractions of U.S. Government Information**

Report all compromises of both U.S. and foreign CMI and unauthorized access to CUI. Personnel must understand these requirements are to ensure US Army responsibilities under Executive Order 12958 are executed properly.

**D-2. Reporting Compromises of Classified Information.** Any USAFCoEFS personnel aware of known or suspected compromises of US or foreign government CMI must notify the Security & Intelligence Division (S&ID), DPTMS immediately and make initial notifications in accordance with DoD Regulation 5200.1-R, Information Security Program, and AR 380-5, Department of the Army Information Security Program.

**D-3. Reporting Unauthorized Access to CUI.** Any USAFCoEFS activity aware of known, or suspected, unauthorized access to CUI by a foreign government, international organization or their representative must notify the FDO, or S&ID, immediately. Notifications will identify where the access occurred, specific information accessed, individual, group or organization permitting access, facts and circumstances surrounding the unauthorized access, and impact of the unauthorized access on the US.

**APPENDIX A  
REFERENCES**

AR 380-10. Foreign Disclosure and Contacts with Foreign Representatives, 22 Jun 05

AR 381-12. Threat Awareness and Reporting Program, 4 Oct 2010

AR 380-5. Department of the Army Information Security Program, 29 Sep 00

AR 25-2. Information Assurance (\*RAR 001, 23 Mar 09), 24 Oct 07

TRADOC Regulation 350-70, Chapter I-1, Systems Approach to Training Management, Processes and Products, 9 Mar 99

AR 12-15. Joint Security Assistance Training (JSAT), 5 Jun 00

**APPENDIX B  
GLOSSARY**

**Section 1  
Abbreviations**

**ADTLP** - Armywide Doctrinal and Training Literature Program

**ARCIC** – Army Capabilities Integration Center

**CLO** – Country Liaison Officer

**CMI** – Classified military information

**CofS** – Chief of Staff

**CO** – Contact Officer

**CUI** – Controlled unclassified information

**DDL** – Delegated Disclosure Authorization Letter

**DoD** – Department of Defense

**FCoE** – Fires Center of Excellence

**FDO** – Foreign Disclosure Officer

**FDR** – Foreign Disclosure Representative

**FLO** – Foreign Liaison Officer

**FVS** – Foreign Visit System

**HQDA** – Headquarters, Department of the Army

**IA** – Information Assurance

**IS** – Information Systems

**ITO** – Invitational Travel Order

**MI** – Military Intelligence

**MOA** – Memorandum of Agreement

**MOU** – Memorandum of Understanding

**NDP-1** – National Disclosure Policy

**OCA** – Original Classification Authority

**ODCS** – Office of Deputy Chief of Staff

**OPSEC** – Operations Security

**PAO** – Public Affairs Officer

**PEP** – Program Exchange Personnel

## USAFCoEFS Regulation 380-10, 01 March 11

**RFI** – Request for information

**RVA** – Request for visit authorization

**SAEDA** – Subversion and Espionage Directed Against the U.S. Army

**SALO** – Security Assistance Liaison Officer

**SME** – Subject matter expert

**STANREP** – Standardization Representative

**SVCO** – Site visit Contact Officer

**TARP** - Threat Awareness and Reporting Program

**TRADOC** – Training and Doctrine Command

**TTPs** - Tactics, techniques and procedures

**USAFCoEFS** – US Army Fires Center of Excellence and Fort Sill

### Section II

#### Terms

As used in this regulation, the following terms apply:

**CLASSIFIED MILITARY INFORMATION (CMI).** Military information, designated by DoD, requiring protection in the interests of national security. CMI will be treated as a national security asset that may only be shared with foreign governments when there is a clearly defined benefit to the US. The information is arranged into three classifications: TOP SECRET, SECRET and CONFIDENTIAL. For brevity, specific categories have been excluded from this document. Information on the eight categories of CMI can be obtained by reviewing DoD Directive 5230.11, dtd June 16, 1992.

**CONTACT OFFICER.** A DoD official (not a contractor) designated in writing to oversee and control all contacts, requests for information, consultations and other activities of foreign representatives (FLOs, EOs, visitors, etc.) who are assigned to, or are visiting, a DoD component or subordinate organization. In the case of personnel exchange programs (EOs), the host supervisor may be the Contact Officer.

**CONTROLLED UNCLASSIFIED INFORMATION (CUI).** Unclassified information of such sensitivity as to warrant a degree of control over its use and dissemination. It is usually consigned to one or more of the following categories:

- Information subject to the Privacy Act of 1974 or otherwise exempt from mandatory disclosure outside the U.S. Government under AR 25-55. This information usually qualifies for application of the marking FOR OFFICIAL USE ONLY.
- Technical information related to research, development, engineering, test, evaluation, production, operation, maintenance, or employment of military

## USAFCoEFS Regulation 380-10, 01 March 11

equipment systems and that, if disseminated outside the U.S. Government, would be subject to export control as outlined in AR 380-10.

*Note:* Coordination is required with local FDO/FDR prior to release.

**DELEGATION OF DISCLOSURE AUTHORITY LETTER (DDL).** A letter issued by the appropriate designated disclosure authority explaining classification levels, categories, scope, and limitations of information that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities. DDLs are **FOR OFFICIAL USE ONLY** and are not releasable to foreign representatives or their parent government.

**DISCLOSURE.** The approved conveyance of CMI or CUI via oral and/or visual transmission of information through approved channels to an authorized representative of a foreign government or international organization. The documents must remain in positive US control at all times. Positive control being the physical or observable possession of CMI during the presence of non-US authorized official or non-secure area.

**FALSE IMPRESSION STATEMENT.** Release of this information in does not imply any commitment or intent on the part of the U.S. Government to provide any additional information on any topic presented herein. This briefing is provided with the understanding that the recipient government will make similar information available to the U.S. Government upon request.

**FOREIGN NATIONAL.** All persons other than US nationals.

**FOREIGN DISCLOSURE OFFICER (FDO).** An individual designated in writing with the authority and responsibility to oversee and control coordination of specific disclosure of CMI and CUI.

**FOREIGN DISCLOSURE REPRESENTATIVE (FDR).** Officials specifically trained and designated in writing that are subject matter experts in their respective areas who advise the FDO on the sensitivity of certain types of information. FDRs do NOT have release authority.

**INTERNATIONAL ORGANIZATION.** An international body, civilian or military, that may have a requirement for access to US CMI or CUI in carrying out its assigned responsibilities.

**MILITARY INFORMATION.** Information under the control or jurisdiction of DoD or of primary interest to them. Military information may be embodied in equipment or may be written, oral or other form.

**NATIONAL DISCLOSURE POLICY (NDP-1).** NDP-1 promulgates national disclosure policy and procedures in the form of specific disclosure criteria and limitations, definitions of terms, release arrangements, and other guidance required by US

ATZR-CS

  
DANIEL L. KARBLER  
COL, GS  
Chief of Staff

James A. Miller  
Director  
Directorate of Human Resources