

BY ORDER OF THE
COMMANDER

HEADQUARTERS, UNITED STATES FORCES, JAPAN
USFJ INSTRUCTION 90-301



01 September 2003

Command Policy

FOREIGN EXCHANGES AND
DISCLOSURE PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ USFJ/J2 (Capt L. Kruger)
Supersedes: HOI 14-301, 8 May 2000

Certified by: CAPT Lendall S. Knight
Pages: 30
Distribution: All USFJ Staff and
Component Commands

PURPOSE: To establish policy and procedural guidance for the disclosure of Classified Military Information (CMI) to foreign governments and international organizations in accordance with all applicable regulations.

SUMMARY OF CHANGES: This revision expands USFJ HOI 14-301 into a USFJ Instruction applicable to a wider base. It creates the USFJ Foreign Disclosure Council and reorganizes the USFJ Foreign Disclosure Board, new staff structures for managing the release or disclosure of Classified Military Information to foreign governments and international organizations. It establishes procedures for Foreign Liaison Officers, a command training plan and checklist for establishing component foreign disclosure programs.

1. **Scope.** This instruction applies to all United States Forces Japan staff, Japan-based U.S. service components and assigned units or elements operating in Japan.

2. **General.**

2.1. It is the policy of the United States Government to treat CMI as a national security asset that must be conserved and protected, and be shared with foreign entities when there is a clearly defined advantage to the United States.

2.2. Basic guidelines for disclosure are contained in the Department of Defense (DoD) National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1) (See Reference A1 in Attachment 1 to this instruction).

2.3. The National Disclosure Policy Committee (NDPC) is the central authority for the formulation, promulgation, administration, and monitoring of NDP-1. References A2-A5 govern implementation of NDP-1 for DoD.

2.4. This instruction does not address coordinating U.S. Freedom of Information Act (FOIA)/ Japanese Freedom of Information Law (JFOIL) requests/responses with the US Embassy or the Government of Japan (GOJ). This program is addressed in USFJ Instruction 37-132.

3. **References.** See Attachment 1 to this instruction.

4. **Definition of Terms.**

4.1. **Classified Military Information (CMI).** Military information designated by Department of Defense (DoD), requiring protection in the interest of national security. The information is limited to three classifications: TOP SECRET, SECRET, and CONFIDENTIAL. CMI is divided into the following categories:

4.1.1. Category 1: Organizational, Training and Employment of Military Forces. Military information of a general nature necessary to the organization of military, paramilitary, or irregular forces to include those tactics, techniques and tactical doctrine (including military intelligence and counterintelligence doctrine and techniques) necessary to train and employ forces.

4.1.2. Category 2: U.S. Military Materiel and Munitions. Includes systems in service (but not under development) and the training to operate and maintain them. Does not include technical data to produce them.

4.1.3. Category 3: Applied Research and Development Information. CMI resulting from the extension of fundamental theories, designs, and data derived from purely theoretical experimental investigations into possible military applications. To include the research, construction, testing of prototypes, and design changes effecting qualitative performance as may be required during the service life of an item. This also includes engineering data, general operational requirements, concepts and military characteristics required to adopt the item for production.

4.1.4. Category 4: Production Information. Consists of the technical data to produce material of U.S. origin. All classified disclosures require an exception to policy.

4.1.5. Category 5: Combined Military Operations, Planning and Readiness. Applies to U.S./foreign government military operations and joint/leased installations.

4.1.6. Category 6: U.S. Order of Battle. Information pertaining to U.S. forces located within territory, which is under the jurisdiction of a recipient government or is otherwise a direct concern to a foreign government or an international organization.

4.1.7. Category 7: North American Defense. Plans and related documents prepared by combined United States / Canada defense agencies. *(Not applicable to USFJ)*

4.1.8. **Category 8: Military Intelligence.** Comprises information of a military character pertaining to foreign nations.

4.2. **Release.** The approved conveyance of CMI in documentary form through approved channels to an authorized representative of a foreign government or international organization. Documentary release refers to the physical release of a document, e-mail, film, recording, tape, electronic disk, card deck, etc.

4.3. **Disclosure.** The approved conveyance of CMI via oral and/or visual transmission of information, through approved channels to an authorized representative of a foreign government or international organization.

4.4. **Coordinating Authority.** A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more military departments or two or more forces of the same service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement.

4.5. **Foreign Disclosure Officer (FDO).** An individual who is designated in writing and who may approve or deny the disclosure of Classified Military Information (CMI) to specified foreign governments and international organizations in accordance with the provisions of the National Disclosure Policy (NDP-1) or exceptions thereto. Disclosures may only be authorized provided disclosure authority has been delegated and has been approved for release by the originating department or agency.

4.6. **Foreign Disclosure Representative (FDR).** An individual appointed in writing who assists the command FDO on all disclosure matters in FDR's respective areas related to administrative, operational, logistical, communications, and intelligence. FDRs are not authorized to release or disclose data to Foreign Nations/Governments.

4.7. **Foreign Disclosure Board (FDB).** The organization that assembles key Foreign Disclosure Representatives and subject matter experts from the staff to address routine operations of the Foreign Exchanges and Disclosure Program. Items that cannot be resolved by the FDB will be forwarded to the Foreign Disclosure Council.

4.8. **Foreign Disclosure Council (FDC).** The Foreign Disclosure organization made up of the Directors assigned to the Headquarters, USFJ. The FDC is not intended to meet on a regular basis, only to address actions referred by the FDB or makes major decisions on USFJ Foreign Disclosure Policy.

4.9. **Foreign National (FN).** All persons other than U.S. nationals.

4.10. **International Organization.** An international body, civilian or military, that may have a requirement for access to U.S. CMI in accomplishing its assigned responsibilities.

4.11. **Uni-Service Intelligence.** That intelligence for which responsibility (cognizance) resides exclusively with a single service.

4.12. **Classification Control Markings.** Terms such as REL TO, ORCON, IMCON, etc which in addition to its classification, intelligence information and certain scientific or technical information may also be subject to other controls on its distribution and handling. A full up to date list of authorized control marking can be found on the Controlled Access Program Coordination Office (CAPCO) SIPRNET homepage at <http://www.cms.cia.sgov.gov/capco/>.

4.13. **Controlled Unclassified Information (CUI).** Unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations and require some form of protection but are outside the formal system for classifying national security information. It could include information that has been declassified, but remains controlled. CUI includes For Official Use Only and information with comparable designations that is received from other agencies, DoD Unclassified Controlled Nuclear Information, "Sensitive Information" as defined in the Computer Security Act of 1987, and DoD technical data.

4.14. **Law Enforcement Agency Sensitive (LEA SENSITIVE).**

4.14.1. Information and materials involving DoD support to Domestic Law Enforcement Agency (DLEA) are considered FOR OFFICIAL USE ONLY (FOUO) information unless the requesting law enforcement agency requires that the information be protected and marked as LEA SENSITIVE (LEAS). To the maximum extent possible, LEAS information will be transmitted via secure means, stored in a locked container, disseminated only when the need-to-know of the recipient has been established, and shredded when no longer required.

4.14.2. LEAS information may be processed on unclassified computers and local area networks. Data will not be stored on a system accessible via the Internet that does not have approved firewall protection. The treatment of this information within DoD channels is not meant to prevent the exchange of this information between DoD units and the originating LEA. In the event the originating LEA does not have secure storage or transmission capabilities, the information may be transmitted over unsecured facsimile machines and stored in locked containers. Within DoD documents, each page, paragraph, and section will be marked in accordance with Attachment 1, Reference A1 and this instruction.

4.14.3. Information on DoD Counter Drug (CD) operations within the United States is generally considered as FOR OFFICIAL USE ONLY, but may be marked LEAS, as determined by the originating agency.

4.14.4. Based on current CD missions, DoD units will not normally originate LEAS information (with the exception of the imagery-derived Gridded Reference Graphic).

However, DoD units will use LEAS protective markings on DoD documents that include such information.

4.15. Drug Enforcement Administration Sensitive (DEAS). A term used to identify sensitive information provided and marked by the DEA. The authority to designate or release information, material, and/or media as DEAS is limited to country attaches, special agents in charge, resident agents in charge, group supervisors and those higher in the field, laboratory chiefs, and representatives occupying supervisory and liaison positions. Information is not releasable outside of DoD channels or to foreign governments without the express permission of the DEA. Items will be stored and mailed using the same methods required for information at the confidential classification level and transmitted by secured communication facilities. Originators of DoD reports containing DEA information must obtain DEA authority to release information outside DoD/DEA channels.

4.16. Unauthorized Disclosure or Release. The oral, visual, or physical act of providing CMI without proper and prior approval.

5. Policy.

5.1. Management of the USFJ Foreign Exchanges and Disclosure Program (FEDP) is the responsibility of the USFJ Director of Intelligence, who appoints a Command Foreign Disclosure Officer (FDO) charged with daily management of the command's Foreign Disclosure Program. The FDO is responsible for promulgating policy changes and serves as the chairman of the USFJ Foreign Disclosure Board (FDB) (see Attachment 5).

5.2. Each USFJ directorate and special staff section will appoint a person (military or civilian) on additional duty to serve as a Foreign Disclosure Representative (FDR). FDRs are the directorates' and special staff sections' members on the FDB.

5.3. The USFJ Chief of Staff is the Chairman of the USFJ Foreign Disclosure Council (FDC) (see Attachment 6). The FDC receives recommendations on USFJ policy from the FDB and determines changes to USFJ Foreign Disclosure Policy. When necessary, proper coordination with the USFJ FDO and the FDB will be conducted.

5.4. All U.S. CMI will be treated as a national security asset which must be conserved and protected, and which may be shared with foreign entities only when there is a clearly defined benefit to the United States.

5.5. Disclosure and denials of CMI will be made only by FDOs specifically granted disclosure or denial authority and after a determination has been made that all of the requirements of NDP-1 have been met.

5.6. Disclosure and release policy as defined in this instruction pertains only to CMI that meets the disclosure criteria stipulated in NDP-1. NDP-1, alone, is not substantive authority to disclose CMI.

5.7. Japan based service components, deployed forces and Joint Task Force Commanders derive disclosure authority from USPACOM as authorized by JCS SM-288-84 and USPACOM INST 5510.3F.

6. USFJ Responsibilities.

6.1. The USFJ Chief of Staff (J02) serves as the chairman of the Foreign Disclosure Council (FDC).

6.2. Director of Intelligence (J2) shall:

6.2.1. Serve as a member of the command's FDC.

6.2.2. Appoint, in writing, a primary and alternate designated disclosure official to serve as the FDO for USFJ. The FDO will chair the FDB.

6.2.3. Ensure the FDO receives training prior to assuming duties and maintains the proficiency required to execute the unit's Foreign Disclosure Program. The following training classes are required at a minimum: Office of the Secretary of Defense, International Programs Security Requirements Course (OSD/IPSR), Chairman of the Joint Chief of Staff, Foreign Disclosure Course for Operators Course (JCS/FDCO), Defense Intelligence Agency, Foreign Exchanges and Disclosure Course (DIA/DPF-2).

6.3. All other USFJ directors and chiefs of special staff sections shall:

6.3.1. Serve as a member of the command's Foreign Disclosure Council.

6.3.2. Appoint, in writing, primary and alternate FDR, who will serve as a member on FDB and manage their respective National Disclosure Policy (NDP) Category 1-8 requirements. A copy of the FDR appointment memorandum will be provided to FDO.

6.3.3. Ensure FDR receives training from USFJ's Foreign Disclosure Office prior to assuming duties and maintains the proficiency required to execute the unit's Foreign Disclosure Program. Additional training by national level organizations through resident classes or Mobile Training Teams, i.e., Office of the Secretary of Defense, International Programs Security Requirements (OSD/IPSR), Chairman of the Joint Chief of Staff, Foreign Disclosure Course for Operators (JCS/FDCO), Defense Intelligence Agency, Foreign Exchanges and Disclosure Course (DIA/DPF-2), and, when available, appropriate service schools, is highly recommended.

6.4. The USFJ Foreign Disclosure Officer (FDO) shall:

6.4.1. Develop command foreign disclosure policy and make recommendations to the Foreign Disclosure Council IAW procedures outlined in Attachment 6.

6.4.2. Develop USFJ foreign disclosure procedures, guidance, and training. Determine requirements for foreign disclosure execution and coordinate implementation as appropriate.

6.4.3. Execute day-to-day Foreign Disclosure operations as they relate to foreign disclosure. Coordinate with USFJ staff and component commands to ensure appropriate administration of policy. Serve as USFJ's single point of contact (POC) to interagency working groups and other commands for all matters affecting the Foreign Exchange and Disclosure Program (FEDP).

6.4.4. Develop specific detailed Foreign Disclosure guidance specific for all bilateral operations or exercises and ensure that the guidance is disseminated in a message to all participants.

6.4.5. Establish and chair the USFJ Foreign Disclosure Board IAW procedures outlined in Attachment 5. The FDRs will consist of the following voting members: FDO, Primary Staff FDRs and selected Special Staff Representatives based on topics and categories of CMIs at issue.

6.4.6. Approve the release of all first time disclosure of CMI. The FDO will coordinate FDR's review of proposed disclosure cases. Where FDR's review results in unanimous concurrence for Categories 1-7, the command FDO signs out the release as approval authority. The FDO alone has authority to sign out the release of CAT 8, Military Intelligence. Where Board FDR's review results in dissenting recommendations, command FDO will refer ENDP case for review/vote to the FDC, whereby final results will be approved.

6.4.7. Serve as an advisor to the FDC. Responsibilities include presenting decision briefings to the officers of the Council and serving as the Council OPR.

6.4.8. Train FDRs and staff personnel involved in Foreign Exchange and Disclosure.

6.4.9. Coordinate with FDOs assigned to USFJ component commands to ensure compliance with procedures and practices outlined in this instruction.

6.4.10. Represent USFJ and Japan based components at the yearly Worldwide Foreign Exchange and Disclosure Conference.

6.5. USFJ Foreign Disclosure Representatives shall:

6.5.1. Develop and maintain written Standard Operating Procedures (SOP) for foreign disclosure of CMI in their respective categories. These SOPs will be reviewed and approved by the USFJ FDO prior to publishing on the USFJ Directorate homepages.

6.5.2. Serve as a member of the FDB. Voting members are listed in Attachment 5.

6.5.3. Coordinate with the USFJ FDO on their respective foreign disclosure issues.

6.5.4. Serve as the single point of contact for their directorate or staff section on foreign disclosure issues.

6.5.5. Serve as the technical advisor to the FDC on issues pertaining to their Directorate.

6.6. Office of Primary Responsibility for Categories of CMI are:

6.6.1. Category 1 (Organization, Training and Employment of Military Forces): J3 FDR.

6.6.2. Category 2 (Military Materiel and Munitions): J5 FDR.

6.6.3. Category 3 (Research and Development Information and Materiel): J5 FDR.

6.6.4. Category 4 (Production Information): J5 FDR.

6.6.5. Category 5 (Combined Military Operations Planning and Readiness): J3 FDR.

6.6.6. Category 6 (U.S. Order of Battle): J3 FDR.

6.6.7. Category 7 (North American Defense): NORTHCOM

6.6.8. Category 8 (Military Intelligence): J2 FDO.

6.6.9. For Plans and Policy portions of Categories 1, 5, and 6: J5 FDR.

6.6.10. For Communications portions of Categories 1 through 6: J6 FDR.

6.6.11. For Personnel Issue portions of Categories 1, 5, and 6: J1 FDR.

6.6.12. For Special Category (SPECAT) portions of Categories 1, 5, and 6: J3 FDR leads with FDO assist.

6.7. USFJ Components, JTFs, and Japan based units involved in foreign exchange or disclosure shall:

6.7.1. For components not already tasked, appoint, in writing, a FDO. Ensure FDO receives training prior to assuming duties and maintains the proficiency required to execute the unit's Foreign Disclosure Program. Training by national level organizations, i.e., Office of the Secretary of Defense, International Programs Security Requirements (OSD/IPSR), Chairman of the Joint Chief of Staff, Foreign Disclosure Course for

Operators (JCS/FDCO), Defense Intelligence Agency, Foreign Exchanges and Disclosure Course (DIA/DPF-2), and appropriate service schools, is highly recommended. The USFJ FDO will assist in training whenever necessary.

6.7.2. Establish and implement foreign disclosure policy, procedures, and practices in compliance with National Disclosure Policy, their respective service policies, and USFJ instructions. Use Attachment 3, USFJ Inspection Checklist, Foreign Exchanges and Disclosure, in developing unit Foreign Disclosure instructions and regulations.

6.7.3. Provide guidance and training to subordinate elements for execution of the command's Foreign Disclosure Program.

6.7.4. Ensure that all Foreign Disclosure guidance issued by USFJ is forwarded to all component organizations involved in bilateral exchanges.

7. General Procedures.

7.1. Prior to any disclosure or release to Foreign Nationals, Foreign Governments or Foreign Organization; any classified and controlled unclassified product must be reviewed by the respective FDO and FDR. The goal is to provide timely and concise recommendations for the disclosure or release of U.S. Military Information to foreign entities (Partner Nation, Coalition) in support of the United States Pacific Command's theater strategy and operations. Unclassified material must be reviewed to ensure no embarrassment to U.S. Government (i.e. Friends on Friends, Political Sensitivity, Copyright, Proprietary Information, Regional Customs, and Commercial Imagery).

7.2. Documents containing CMI that originated outside USPACOM, even though they bear no control markings, will not be released in their original form to foreign governments or international organizations without permission of the originator. The only exception is IAW Attachment 1, A8, Category 8 CMI that bears no control markings may be used in other classified finished intelligence documents and disseminated as the producer of the intelligence deems appropriate and necessary. Dissemination may include release to foreign governments under the provisions of this instruction. The information, however, must be extracted or paraphrased and used within the text in a manner that effectively conceals the identity of the originating agency, the source, the place and date acquired, and the manner of acquisition. If disclosure is made to a foreign government, no reference shall be made to the document from which the finished intelligence is drawn.

7.3. One-time disclosure requests by foreign governments and international organizations for U.S. CMI and/or U.S. generated disclosure proposals, will be processed as follows:

7.3.1. Uni-Service disclosure requests originated by USPACOM component commands will be processed within the appropriate Service channels. USFJ will serve as the overall Coordinating Authority for Category 8 issues. (see Attachment 1, Reference A19, USFJ Instruction 14-102).

7.3.2. USPACOM JTFs based in Japan request for disclosure will be processed through USPACOM to the appropriate service Joint Staff.

7.3.3. All proposed/planned disclosures that require coordination with the USFJ FDO shall be submitted by email or hard copy and shall include the following information:

7.3.3.1. Serial Number/Title/Date/Classification of document;

7.3.3.2. Agency that produced the source document;

7.3.3.3. Identity of the intended recipient(s)/government agency to whom information will be disclosed;

7.3.3.4. The method of proposed disclosure (oral, visual, or documentary);

7.3.3.5. A complete identity or transcript of the information to be disclosed (NOTE: Each paragraph or portion of the transcript, briefing, text, etc., will identify the classification, restrictive marking, if any, and the source of information);

7.3.3.6. The justification and “need-to-know” on the part of the proposed recipient(s);

7.3.3.7. The expected benefits that would accrue to the United States;

7.3.3.8. Date release/disclosure is required

7.3.3.9. The specific authority that allows the proposed/planned disclosure. Authority is delegated from higher headquarters via regular message traffic or official instruction.

7.4. Delegated Authority. USFJ Staff, Component, and Joint Task Force Commanders will be authorized to disclose U.S. classified military information to those allied or other partner foreign governments and international organizations located in their assigned geographic area of responsibility as directed by USPACOM. This provision is limited to military information specified in Attachment 1, Reference A7. This authority may not be further delegated.

7.5. Emergency Delegation of Release Authority (EDA). Pending imminent commencement of hostilities, CDR USPACOM retains Proper Authority (PA) and EDA for the sanitization and release of specialized intelligence products. In the event of hostilities, CDR USPACOM may delegate PA and EDA to component, sub-unified, and Joint Task Force commanders. DOD-5105/21-M-2 requires PA be delegated in writing. CDR USPACOM will promulgate messages formally delegating PA and EDA.

7.6. Senior Foreign Official Requests. Senior Foreign Official requests will be processed IAW Attachment 1, Reference A6. Staffing procedures include a written request specifying the name(s) of the foreign official(s), the date he/she is briefed, information to be briefed, and classification of the information. The USFJ FDO will

forward these requests to the USPACOM and Defense Intelligence Agency Foreign Disclosure Office, which require at least ten working days each for coordination.

7.7. Special Category CMI. Procedures for the release of Special Category (SPECAT) CMI do not differ from the requirements for the release of collateral CMI. All USPACOM originated CMI will be protected to the fullest extent of this instruction, NDP-1, and CJCSM 3213.02A. When USFJ staff, components, or joint task forces desire to release or deny SPECAT CMI to a foreign government, a request action will be forwarded to the USFJ FDO for command resolution. SPECAT action requests and historical files will be protected and maintained separate from collateral CMI.

7.8. Procedures for the release of Narcotics Intelligence (NARCINT) differ from the requirements for release of CMI in that approval for release from U.S. Embassy Country Team must be accomplished before information is released. All USPACOM originated NARCINT will be protected in accordance with this instruction, NDP-1, CJCSM 3701.01A, and DPF-0000-217-99-DIAM. NARCINT action requests and historical files will be protected and maintained separate from CMI. NOTE: Procedures for the release of Imagery Intelligence (IMINT) for counter drug operations differs from the requirements for release of other CMI in that approval for release for different categories of IMINT resides with specific agencies. The Director for Central Intelligence Agency is the sole release authority for national satellite imagery. Director of Defense Intelligence Agency is the release authority for National and DoD air-breather imagery. USPACOM is release authority for theater imagery.

7.9. Inadvertent disclosure or the compromise of classified information can present a threat to national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action should also be taken to regain custody of documents or materials that were compromised. In all cases, appropriate action must be taken to identify the source and reason for the actual or potential compromise and remedial action to be taken to prevent recurrence. Anyone finding classified material out of proper control shall take custody of and safeguard the material, if possible, and immediately notify the appropriate security authorities. Any person who becomes aware of the possible compromise of classified information shall immediately report it to the head of his or her local activity or to the activity security manager. If the person believes that the head of the activity or the security manager may have been involved in the incident, he or she may report it to the security authorities at the next higher level of command or supervision.

7.9.1. Actual or potential compromises involving cryptologic information shall be handled in accordance with NACSI 4006.

7.9.2. Actual or potential compromises involving SCI will be handled in accordance with DoD S-5105.21-M-I, and reported to Special Security Officer.

7.10. Requests for exception to any policies outlined in this instruction must be justified in writing to the USFJ FDO for approval.

8. Procedures for Foreign Visitors to USFJ Facilities.

8.1. Official foreign visit requests are not required for visits to USFJ bases by Japanese military and government officials for the course of normal duties. All release or disclosure of CMI will be conducted only with proper authority and when all of the requirements of NDP-1 have been met.

8.2. Visits by military or government officials from other than the Government of Japan (including representatives of a foreign interest or non-government organizations (NGOs) to USFJ bases will be limited to unclassified information, unless disclosure of CMI for that visit has been authorized by respective FDO, and this instruction. Visits by United Nations Command (UNC) Rear bases by member nations will occur in accordance with UNC procedures and delegated authorities.

8.3. Visits to CONUS sites sponsored by the Japanese government may occur only after the following conditions are met:

8.3.1. GOJ requests visit authorization from their embassy in Washington, D.C.

8.3.2. GOJ's embassy forwards all appropriate documentation to DIA Foreign Liaison (DIA/PO-FL), including phone number.

8.3.3. DIA/PO-FL submits visit request action memorandum to USPACOM, and requests a memorandum concurring/non-concurring with the visit. USPACOM will coordinate with USFJ or service component regarding approval/disapproval.

8.3.4. The DIA/PO-FL notifies the GOJ's embassy of the approval/disapproval. If the visit is disapproved, no other action is required. If the visit is approved, DIA/PO-FL will forward a copy of the final visit request approval documentation to USPACOM.

8.3.5. If the visit requires access to classified information, the directorate coordinates with the directorate's FDR to confirm the material is releasable.

8.4. For additional information concerning Foreign Visits see Attachment 1, Reference A4.

9. Foreign Liaison Officers

9.1. A Foreign Liaison Officer (FLO) is per Attachment 1, Reference A4 a foreign government military member or civilian employee who is authorized by his or her government, and is certified by a DOD Component, to act as an official representative of that government in its dealings with a DOD Component in connection with programs, projects or agreements of interest to the governments.

9.2. FLOs assigned to USFJ will be conducted in accordance with the guidelines listed below:

9.2.1. All FLOs will have a contact officer assigned in writing who will handle any administration involved in the assignment.

9.2.2. The FLO contact officer will ensure that J06 provides documentation describing the legal status of the proposed FLO (including any privileges and immunities to which the liaison officer is entitled) and sponsoring government responsibilities.

9.2.3. The FLO contact officer must have a statement from the sponsoring government or agency that the proposed FLO is authorized by the sponsoring government to conduct business.

9.2.4. A security assurance statement must be provided to the FLO by the sponsoring government indicating the proposed FLO holds a specified level of security clearance.

9.2.5. A security assurance statement must be provided to the FLO contact officer, signed by the FLO indicating they will protect all U.S. classified or controlled unclassified information in a manner consistent with U.S. laws or regulations.

9.2.6. A statement must be provided to the FLO contact officer by the sponsoring government indicating whether the proposed FLO may assume custody of documentary information on behalf of the sponsoring government.

9.3. FLOs assigned to USFJ will be authorized access to NIPRNET in accordance with policy set forth in Attachment 1, Reference A14 access to NIPRNET. Specifically:

9.3.1. FLO's e-mail account and signature block must identify individuals as foreign officers, including assignment and the country of origin.

9.3.2. FLOs must adhere to local information assurance and computer security procedures and practices. Personnel security assurance and appropriate level investigation is required from the foreign government as specified in Attachment 1, Reference A4.

<SIGNED>

T. R. LARSEN
Brigadier General, U.S. Marine Corps
Deputy Commander

Attachments:

1. References
2. Guidance on Processing Exceptions to National Disclosure (ENDP) Policy
3. USFJ Inspection Checklist for Foreign Exchanges and Disclosure
4. Quick Reference Checklist on Foreign Disclosure
5. USFJ Foreign Disclosure Board
6. Foreign Disclosure Council

Attachment 1 REFERENCES

- A1. National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (Short Title: National Disclosure Policy (NDP-1) (U) (SECRET//NOFORN), 2 October 00.
- A2. DOD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations (UNCLASSIFIED), 16 June 1992.
- A3. DOD Directive 5230.17, Procedures and Standards for Disclosure of Military Information to Foreign Activities (UNCLASSIFIED).
- A4. DOD Instruction 5230.20, Visits and Assignments of Foreign Representatives (UNCLASSIFIED), 12 August 1998.
- A5. DOD Directive 5230.23, Intelligence Disclosure Policy (U) (CONFIDENTIAL), 18 November 1983.
- A6. DIA Regulation, Number 60-33, Approval Procedures for Disclosure of Classified U.S. Intelligence to Senior Foreign Officials (U) (CONFIDENTIAL), 15 January 1987.
- A7. CJCSSI 5221.01A, Delegation of Authority to Commanders of Unified and Specified Commands to Disclose CMI to Foreign Governments and International Organizations, 06 April 1999 (UNCLASSIFIED).
- A8. Director of Central Intelligence Directive (DCID) 6/6, Security Controls on the Dissemination of Intelligence Information (U) (CONFIDENTIAL), 11 July 2001.
- A9. DCID 6/7, Intelligence Disclosure Policy (U) (CONFIDENTIAL), Dated 30 June 1998.
- A10. DIAM-DPF-0000-217-99, DIA Guide to Foreign Disclosure (U) (CONFIDENTIAL//NOFORN//X1), November 1999.
- A11. CJCSM 3701.01A, Classification Guide for Counter drug Information of 25 February 2000 (U) (CONFIDENTIAL//REL TO USA, AUS, CAN, and GBR).
- A12. DIA message, Disclosure of Narcotics Intelligence to Foreign Nationals (U) (SECRET), DTG 211725ZMAR90.
- A13. DIA Memorandum, Narcotics Intelligence Disclosure Policy (U) (CONFIDENTIAL), dated 20 April 1990.
- A14. Joint Staff Message, Foreign Liaison Officer Access to NIPRNET Policy, (UNCLASSIFIED) DTG 021633Z JUL 01.

A15, USPACOM INST C3020K.2K: Command Relationships in the U.S. Pacific Command (USPACOM), (UNCLASSIFIED) 01 June 1993.

A16. USPACOM INST 3824.1E: International Intelligence Relationships, (UNCLASSIFIED) 22 December 2000.

A17. USPACOM INST 5510.3F: USPACOM Policies and Procedures for the Disclosure or Release of Classified Military Information (CMI) to Foreign Governments and International Organizations, (UNCLASSIFIED) 20 May 1989.

A18. USPACOM INST S5510.30, USPACOM Policy and Procedures for the Disclosure or Release of Classified Military Intelligence to the Government of Japan, (U) (SECRET//NOFORN) 13 April 2001

A19. USFJ INST 14-102, Intelligence Sharing (U), (SECRET//NOFORN), 30 Nov 2000.

A20. CJCSI 6510.06, Communications Security Releases to Foreign Nations (For Official Use Only), 15 February 2001

A21. AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, (U) (CONFIDENTIAL) 6 June 2003.

A22. AR 380-11, Maximum Classification Levels for Release in Accordance with the Department of Army Policy for Disclosure of Classified Military Information to Foreign Governments, 15 February 2001.

A23. SECNAV Instruction 5510.34, Manual for the Disclosure of Classified Information to Foreign Governments and International Organizations (UNCLASSIFIED), 4 November 1993.

A24. AFI 200-9, Disclosure of Classified Military Information to Foreign Governments and International Organizations (U) (CONFIDENTIAL).

Attachment 2
GUIDANCE ON PROCESSING EXCEPTIONS TO
NATIONAL DISCLOSURE (ENDP) POLICY

Proposals to disclose Classified Military Information (CMI) which exceed the disclosure criteria for a country must be fully justified and contain the following elements of information:

1. A concise statement of the action proposed. Include security classification and categories of U.S. CMI to be disclosed.
2. A precise statement of why an exception to policy is required. An exception is required because:
 - 2.1. The level of classified information involved exceeds the classification level delegated in Annex A of NDP-1.
 - 2.2. The proposed action is not in consonance with policy currently established in Annex B or C, as applicable, of NDP-1.
 - 2.3. Certain (identify which) of the disclosure criteria or conditions listed in section II. of NDP-1 are not fully met.
 - 2.4. Any or all of the above criteria in combination.
3. An assessment of how each of the disclosure criteria and conditions in section II. Of NDP-1 shall be met:
 - 3.1. Disclosure is consistent with the foreign policy of the United States toward the Government of _____.” (A further detailed discussion shall be included to substantiate this statement. Reference shall be made to Presidential, National Security Council, or other high-level policy decisions to support the justification provided. A simple statement such as “the recipient cooperates with the United States in pursuance of military and political objectives” is not sufficient; how the recipient cooperates is, however, important.)
 - 3.2. “The military security of the United States permits disclosure.” (If equipment or technology is involved, there must be a discussion on the result of a compromise on U.S. operational capability or the U.S. position in military technology. This discussion shall include an analysis of the state of the art regarding the technology involved, the susceptibility of the item to reverse engineering, the capability of the foreign recipient to reverse engineer the item, the foreign availability of the technology or equipment involved, and other governments to whom similar equipment or technology has been released. For other types of information, the value of the information to U.S. defense and/or foreign policy should be described, along with an analysis of likely damage in the event of compromise.)
 - 3.3. “The foreign recipient will afford the information substantially the same degree of security protection given to it by the United States.” (If there has been an NDPC

Security Survey for the proposed recipient, the conclusion reached therein shall be discussed. In the absence of an NDPC Security Survey, efforts shall be made to obtain, through intelligence channels, a counterintelligence risk assessment or security analysis of the foreign government's security capabilities. The mere statement that "classified information has been released previously to this government and there is no indication that such information has been compromised" is not sufficient. If the recipient government's capability and intent cannot be evaluated, so state.)

3.4. "Disclosure will result in benefits to the United States at least equivalent to the value of the information disclosed." (For example: (1) if the United States obtains information from the proposed recipient on a quid-pro-quo basis, describe the information and the value to the United States; (2) explain how the exchange of military information for participation in a cooperative project will be advantageous to the United States from a technical or military capability viewpoint; (3) if the development or maintenance of a high degree of military strength and effectiveness on the part of the recipient government will be advantageous to the United States, explain how.)

3.5. "The disclosure is limited to information necessary to the purpose for which disclosure is made." (For example, if the purpose of the request is for the sale of equipment only, it shall be indicated clearly that research and development data or production know-how is not to be divulged or that documentation will be sanitized. This analysis, together with paragraph 4, below, is the basis for a delegation of disclosure authority letter.)

4. Any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure schedules, or other pertinent caveats that may affect NDPC approval or denial of the request. (If disclosures are to be phased or if certain information is not to be released, the phasing or non-releasable information shall be specified.)

5. A statement that the requested exception is to be either a continuing exception, subject to annual review, or a one-time exception. (A continuing exception usually is associated with a long-term project, such as a co-production 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.) If a one-time exception, indicate an expiration date.

6. The names and titles of U.S. officials accredited to the requesting foreign government or international organization with whom the proposed exception has been coordinated, as well as the views of the Theater Commander. Sufficient time shall be allowed to obtain an opinion from U.S. Embassy personnel in country and the responsible Theater Commander before submitting the request for approval. Many cases are delayed because a U.S. Embassy or Theater Commander opinion has not been obtained.)

7. The opinion of other interested Departments or Agencies if joint Service or shared information is involved. (If the information or item of equipment is 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 will be included.)

8. Any information not mentioned above that would assist the NDPC members, the Secretary of Defense, or the Deputy Secretary of Defense in evaluating the proposal.

9. The name and telephone number of a knowledgeable individual within the requesting organization who can provide additional technical detail or clarification concerning the case at issue.

10. The date a response is desired on the case. 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 the request is received by the NDPC.

Attachment 3
USFJ INSPECTION CHECKLIST
FOREIGN EXCHANGES AND DISCLOSURE

(Checklist subject to update: current list located at
http://www-j2.pass-j.pacom.smil.mil/usfj/j22_e/index.html)

Yes No NA

AUTHORITIES:

1. Does the Foreign Disclosure Officer (FDO)/ Representative (FDR) and the Assistant FDO (AFDO) have an official appointment letter? (NDP-1, 4.f; DIA guide to FD Attachment 6, CJCSI 5221.01 A) ☐ ☐ ☐
2. Has FDO or FDR appointment memorandum been forward to the J2? ☐ ☐ ☐
3. Are there recurring International Agreements (as defined in DoD Directive 5530.3, 11 June 1987), Intelligence Exchange agreements, CISMOA, etc., involving your activity, which requires the release of CMI? ☐ ☐ ☐
 - 3.1. What are those agreements? _____
 - 3.2. Who is the Office of Record? _____
 - 3.3. Where are they maintained? _____
 - 3.4. What are the level, quantity, and frequency of CMI release? _____
4. Does the FDO have a copy of the National Disclosure Policy-1(NDP-1)? ☐ ☐ ☐
5. Does the command exercise any temporary authorities to support special missions? ☐ ☐ ☐
 Note: Support to temporary Coalitions would fall into this category.
6. Does the FDO have the necessary documents and regulations? ☐ ☐ ☐

Note: FDOs should act upon legally delegated authority at all times to include understanding the limits of their respective authority. FDOs will become knowledgeable on the following:

- Where to turn for clarification or interpretation of disclosure policies.
- Where to look first for disclosure assistance.
- How to identify the particular office or agency for petitioning for expansion of their authorities.

- | | <u>Yes</u> | <u>No</u> | <u>NA</u> |
|---|--------------------------|--------------------------|--------------------------|
| 6.1. <u>DIA REG 60-28</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Establishes military intelligence agreement guidelines for Military Exchanges. | | | |
| 6.2. <u>(NSDM) 119 National Security Decision Memorandum</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Note: Disclosure of classified U.S. military information to foreign governments and international organizations. Dated 20 July 1971. 4 pages. This document provides presidential-level approval for the development of a national program to release classified military information (CMI) to foreign governments, and defines CMI as a "national security asset...which may only be disclosed to foreign governments and international organizations when there is a clearly defined advantage to the United States." This document begins the process by which foreign disclosure authority is formally sub delegated to action officers worldwide. | | | |
| 6.3. <u>DCID 6/6 Security Controls on the Dissemination of Intelligence Information</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Security controls on the dissemination of intelligence information. This DCID outlines the policies, control markings, and procedures for disseminating intelligence. | | | |
| 6.4. <u>DCID 6/7 Intelligence Disclosure Policy</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| DCID 6/7 outlines community-level responsibilities, procedures, and criteria for the disclosure of intelligence to foreign governments, international organizations, and coalition partners, including the requirement to keep "permanent and retrievable records" of all foreign disclosures and denials. This DCID also outlines the policy and procedures pertaining to all disclosures to senior foreign officials. Of significance, DCID 6/7 identifies the types of intelligence that may not be disclosed. An important document for anyone engaged in disclosures of category 8 (military intelligence) information. Effective 20 April 2001. | | | |
| 6.5. <u>DoDD 5230.11 Disclosure of Classified Military Information to Foreign Governments and International Organizations</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| This directive implements NDP-1 for all Department of Defense elements, identifying the specific foreign disclosure policies, roles, and responsibilities of certain DoD agencies and offices—such as the Under Secretary of Defense for Policy; the Director, DIA; and the Chairman, JCS—within the overall DoD structure. These responsibilities include: authorizing or denying disclosures of CMI; designating in writing, senior disclosure officials; sub delegating as appropriate, foreign disclosure authority to subordinate elements; and, ensuring the competency of those officials with sub delegated authority. In this regard, DoDD 5230.11 sub delegates from the SECDEF—to DR, DIA; CJCS; and others—the foreign disclosure authority delegated from the President to the SECDEF in NSDM 119. Dated 16 June 1992. 12 pages with 6 enclosures. | | | |
| 6.6. <u>DoDD 5230.18 The DoD Foreign Disclosure and Technical Information System (FORDTIS)</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| This is the regulation that outlines the policies, procedures and responsibilities for DoD components concerning the record keeping for a variety of foreign disclosure matters on | | | |

the FORDTIS system. As the FORDTIS system has application to foreign visits, exceptions to the NDP-1, the transfer of technical data and systems, and other types of foreign disclosure cases. Dated 6 Nov 1984. 4 pages, with 5 enclosures.

6.7. DoDD 5230.20 Visits and Assignments of Foreign Representatives

Yes No NA
☐ ☐ ☐

This regulation speaks to the policies and responsibilities of DoD components where foreign visitors are concerned, as well as where the assignment of foreign nationals to DoD components is concerned. This directive includes guidance concerning one-time visits by foreign personnel as well as for recurring visits, and establishes both the International Visits Program (IVP) and the Defense Personnel Exchange Program (DPEP). Dated 24 April 1992. 5 pages, with 6 enclosures.

6.8. CJCSM 3701.01A Classification Guide for Counterdrug Information

☐ ☐ ☐

Manual incorporates new classification requirements for national security information and revises handling procedures for LAW ENFORCEMENT AGENCY SENSITIVE and DRUG ENFORCEMENT ADMINISTRATION SENSITIVE information.

6.8.1. How many Delegated Disclosure Authority Letters (DDL) have been provided to your activity_____?

6.8.1.1. How often does disclosure occur under this authority and how is it reported_____?

6.8.2. What are your procedures for staffing disclosure requests that exceed the authority of the DDL? _____

6.8.2.1. How often were DDLs exercised last year?_____

6.9. Is your activity the author of any DDLs? ☐ ☐ ☐

7. UNDERSTANDING OF REGULATIONS:

7.1. Does local FDO/FDR seem to understand the limits and parameters of the authority they have been given? ☐ ☐ ☐

8. TRAINING:

- Secretary of Defense, International Programs and Security Requirements (OSD/IPSR)
- Defense Intelligence Agency, Foreign Exchanges and Disclosure Course (DIA/DPF-2)
- Joint Chiefs of Staff, Foreign Disclosure for Operators (JCS/J5)

8.1. Has the FDO and Assistant FDO received proper training and certification?

Yes No NA
☐ ☐ ☐

9. RESPECTIVE SERVICE SCHOOLS:

- U.S. Army Foreign Disclosure Course
- U.S. Air Force Foreign Disclosure Course

9.1. Has the Foreign Disclosure Representative received proper training and certification (USFJ Foreign Disclosure Course)?

☐ ☐ ☐

9.2. Does your activity provide classified training to foreign nationals?

☐ ☐ ☐

9.3. How do you address foreign disclosure concerns?

9.4. How do you provide FD education and training to assigned U.S. personnel on matters related to foreign disclosure?_____.

9.4.1. How often and how is this training documented?

10. RECORD KEEPING:

10.1. How do you maintain control of disclosures of classified military information (CMI) to foreign governments?_____.

10.2. What written procedures or SOPs exist in your organization to support this control?_____. (Refer to SC Reg 380-10 and Respective Service

10.3. Does the FDO/FDR keep an updated log of all releases and disclosures?

☐ ☐ ☐

10.4. How are the disclosure records kept, (i.e. is there a database or hardcopy files)_____?

10.4.1. Is this responsibility divided between divisions of the organization or is it centrally located?_____

11. PROCEDURES:

11.1. Do office procedures support or detract from exchange/disclosure mission?

☐ ☐ ☐

- | | Yes | No | NA |
|--|--------------------------|--------------------------|--------------------------|
| 11.2. Is there an internal SOP or guidance provided? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.3. Are there enough dedicated disclosure officials, given size of the mission? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.4. To what extent do you participate in rendering advice and disclosure guidance to personnel of your command who will give briefings and perform demonstrations, both in the United States and in foreign countries where foreigners will be in attendance?
(Explain) _____ | | | |
| 11.5. To what extent does the FDO/FDR influence the command in the decision whether or not to disclose CMI? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.5.1. Who makes the final decision? _____ | | | |
| 11.5.2. What other entities participate? _____ | | | |
| 11.6. Are any foreign personnel or liaison exchange officers certified or assigned to your activity or under the Defense Exchange Program? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.7. If so, how does the command handle the associated foreign disclosure concerns? _____ | | | |
| 11.8. Is there an MOA on file between the two organizations? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.9. How many requests for non-GOJ foreigners to visit your activity did you receive last year? _____ | | | |
| 11.10. Are there local unit procedures (SOP) in place? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.11. What percentage (of what?) required the disclosure of CMI; or disclosure to Counter-Drug information (NARCINT)? _____ | | | |
| 11.12. Did you require an Exception to National Disclosure Policy (ENDP), for any CMI that was released? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11.13. How many requests for documents were received from foreign governments and international organizations last year? _____ | | | |
| 11.13.1. The year before? _____ | | | |
| 11.13.2. During the last four months? _____ | | | |
| 11.14. What are your activities procedures (protocol) for addressing foreign visitor requests for documentary copies of CMI briefings they received in person? | | | |

11.15. Do you provide imagery products for release to foreign nationals? ☐ ☐ ☐

11.15.1. If so what types? _____

11.16. What types of imagery-derived products are requested of your organization from foreign officials, if any? _____

11.17. What classification guidance do you follow to produce imagery products for release to foreign nationals? _____

11.18. What procedures are in place for you to provide releasable imagery? _____

11.19. What electronic systems are used to transmit releasable information to consumers? _____

11.20. Is there proper security awareness concerning properly marked releasable products being placed on certain electronic systems? ☐ ☐ ☐

Note: In some instances, especially where imagery products are concerned, there may be dissemination limitations tied to the delegations of authority.

11.21. Do documents that are derivatively classified contain a list of sources? ☐ ☐ ☐

11.22. Are transmittal documents properly marked "RELEASABLE TO USA and JPN" on hardcopy or electronically? ☐ ☐ ☐

11.23. Does the FDO/FDR know the difference between LEA and DEA sensitive classification? (CJCSM 3701.01 A) ☐ ☐ ☐

Attachment 4

Quick Reference Checklist on Foreign Disclosure

This checklist is designed to assist the staff in correctly executing foreign disclosure procedures. It neither replaces U.S. law or regulations nor relieves individuals of their responsibility to properly coordinate all foreign disclosure actions. If further assistance is required, contact USFJ Foreign Disclosure Office.

- ❑ Upon notification of a foreign disclosure requirement (to include escorting foreign officials), contact your foreign disclosure representative (FDR) for initial guidance, review, and approval (if applicable). Ensure security manager is contacted to verify classified material clearance level.
- ❑ Upon determination that a classified briefing or intelligence product has been requested, initiate a request through the directorate FDR to the USFJ Foreign Disclosure Officer (FDO). FDO will require at least ten working days prior to the planned presentation to research and verify approval for disclosure (show only).
- ❑ All briefing slides and text must be approved by your FDR prior to presentation to a foreign audience.
- ❑ Ensure each slide/page is labeled, with the appropriate classification marking and releasability information. SECRET//RELEASABLE TO USA and JPN.
- ❑ Ensure each paragraph is labeled appropriately with the proper classification abbreviation and releasability information. S//REL TO USA and JPN or S//REL if the whole document is releasable.
- ❑ NOFORN, ORCON, IMCON, or REL TO any country other than Japan cannot be released without originator approval. Requestor will, in conjunction with unit FDO, coordinate with the originator for a releasable/tear line version of the sanitized product. USFJ FDO can assist as required. Always provide original source and specific reference when requesting release or “tear line” information.
- ❑ Ensure there is no reference to sources or methods. Do not reference specific collection platforms or programs.
- ❑ Do not mention “friends on friends” issues. In addition, do not provide intelligence on a host country to its foreign officials without permission to collect information in country.
- ❑ Do not disclose something that may embarrass the U. S. or one of its allies. Any statement that offends/demeans a host nation, friendly AOR, allied nation, or personality.
- ❑ Be sensitive of religious or regional political issues.

- ❑ Do not reference or provide access to OPLANS, OPORDS, or ROE unless authority has been previously provided for disclosure or release.
- ❑ Try to limit quantitative numbers that reveal specific strength. Instead, use approximations or vague terms such as “numerous” or “undetermined.” For U.S./allied movement dates and schedules, do not use specific dates. Instead, use “EARLY,” “MID,” or “LATE,” especially when used to refer to collection dates.
- ❑ If the source is unclassified, it should still be run through a Foreign Disclosure Review. Your discussion of unclassified data may imply validation.
- ❑ Do not reference gaps in collection or weaknesses of friendly forces.
- ❑ Do not issue statements that could be used as propaganda to support threat organizations.
- ❑ Do not reference Intelligence exchanges with other foreign countries.

Attachment 5
USFJ FOREIGN DISCLOSURE BOARD

1. The Foreign Disclosure Officer (FDO) chairs the Foreign Disclosure Board (FDB). This body assembles key Foreign Disclosure Representatives (FDR) and subject matter experts from the staff to address routine operations of the Foreign Exchanges and Disclosure Program.

2. The FDB meets quarterly as a rule to review issues referred by the FDO/FDRs. The FDB may meet more often as requested and coordinated by the USFJ FDO. The FDB reviews and develops command policy, subject to the approval of the FDB. The Council also reviews ENDP requests and makes recommendations to the USPACOM FDO. When the Council reaches consensus on requests, the FDO may sign out the action without further review from the command group or FDB. When the council is unable to reach consensus or its recommendations result in policy change, the FDO will request that the FDC convene and render a decision.

3. Voting membership of the FDB:

<u>USFJ Staff Representative</u>	<u>Position</u>
Command FDO (J2)	Chairman
J1 FDR	Member
J3 FDR	Member
J4 FDR	Member
J5 FDR	Member
J6 FDR	Member
J023 FDR	Member

4. FDRs from other staff sections are encouraged to participate in council proceedings as non-voting members.

Attachment 6
FOREIGN DISCLOSURE COUNCIL

1. The Chief of Staff chairs the Foreign Disclosure Council (FDC). This body assembles all Directors assigned to the Headquarters, USFJ to address actions referred by the Foreign Disclosure Board (FDB) or to make decisions on USFJ Foreign Disclosure Policy
2. The FDC meets as necessary and is determined by the Chief of Staff to review issues referred by the FDB for Director consideration.
3. The FDC is made up of the following personnel:

USFJ Representative	Position
Chief of Staff	Chairman
J1	Member
J2	Member
J3	Member
J4	Member
J5	Member
J6	Member
J023	Member
J06	Member
Command Foreign Disclosure Officer (J2)	Recorder

Attachment 7 USFJ FOREIGN DISCLOSURE FLOW DIAGRAM

