CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

DOM/JSSO CJCSM 5230.01A
DISTRIBUTION: A, B, C, JEL 21 December 2017

JOINT STAFF FOREIGN DISCLOSURE AND FOREIGN VISITS PROGRAMS

References: See Enclosure F

1. Purpose. The purpose of this manual is to provide policy and procedural guidance for disclosure of classified military information (CMI) to foreign governments and international organizations and for management and operation of the Foreign Visits Program at the Joint Staff and at the headquarters of the Combatant Commands (CCMDs). The National Security Strategy of the United States stresses that the "imperatives of engagement" in the world are vital for our security. To achieve our security objectives, the United States must remain the preferred security partner for the community of states that share our interests. Foreign disclosure and technology transfer are key and essential to successfully executing a strategy of engagement.

2. Superseded/Cancellation. CJCSM 5230.01, 23 April 2014, "Joint Staff Foreign Disclosure and Foreign Visits Programs" is hereby superseded.

3. Applicability. This manual applies to all personnel employed or attached to the Joint Staff, including contractors and consultants. It also applies to the CCMDs and the Defense Intelligence Agency (DIA) for functions in which they are responsive to the Chairman of the Joint Chiefs of Staff. Other agencies should consult this manual when they desire to disclose Joint Staff owned/originated CMI to foreign governments or international organizations. Control of disclosure of Controlled Unclassified Information (CUI) is not governed by foreign disclosure policy but by policy related to the particular type of information, and will be a subject of other guidance.

4. Procedures. Enclosures C, D, and E provide detailed procedural guidance for Joint Staff and CCMD personnel to ensure that foreign disclosure and foreign visit functions are performed in accordance with requirements defined in the references in Enclosure F.

5. Summary of Changes. Adds new disclosure information and directions for disclosure of Intelligence information via the Joint Staff J2/DIA.

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. DoD Components (to include the CCMDs), other Federal Agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at <http://www.jcs.mil/library>. JS activities may also obtain access via the SIPR JS Directives Electronic Library web site.

7. Effective Date. This MANUAL is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

KENNETH F. MCKENZIE, JR.
LtGen, U.S. Marine Corps
Director, Joint Staff

ENCLOSURES:

A - General Information and Policy
B - Roles and Responsibilities
C - Foreign Disclosure Procedures
D - Foreign Visits Procedures
E - Requests for Exception to National Disclosure Policy
F - References
GL - Glossary

TABLE OF CONTENTS

ENCLOSURE A GENERAL INFORMATION AND POLICY

ENCLOSURE A

GENERAL INFORMATION AND POLICY

1. General Information. Foreign disclosure is the process by which classified information is made available through approved channels to an authorized representative of a foreign government or international organization. There are three disclosure methods: oral, visual, and documentary. Documentary disclosures result in transmission of classified information in any written or recorded format. Release is disclosure of classified information through transfer of some concrete item, including a document. Only designated disclosure authorities, specifically appointed in writing by individuals already having written foreign disclosure authority, have the authority to approve disclosure or release of CMI to foreign governments or international organizations.

2. Tenets of Foreign Disclosure

a. Strict controls are placed on disclosure and release of CMI:

(1) There must be a clear benefit to the United States.

(2) The intended recipient must be eligible to receive CMI.

(3) The recipient must have Need-to-Know.

(4) Foreign representatives must have commensurate foreign personnel security clearances.

(5) The recipient must provide protection of information equivalent to U.S. protection.

(6) Reciprocal security arrangements must be in place.

b. U.S. personnel requirements:

(1) Must have written authority to release or disclose CMI.

(2) Must be the proper channel for disclosure of the information.

c. It is the policy of the United States to avoid creating false impressions of U.S. willingness or readiness to make available or otherwise disclose/release classified military information, materiel, or technology.

3. Policy

a. It is the policy of the U.S. Government to treat CMI as a national security asset, which must be conserved and protected, and which may be shared with foreign governments and international organizations only when there is a clearly defined advantage to the United States. The basic National Disclosure Policy (NDP-1) is contained in reference a. The National Disclosure Policy Committee (NDPC) is the central authority for formulation, promulgation, administration, and monitoring of NDP-1. Reference b implements NDP-1 for the Department of Defense.

b. The Chairman's foreign disclosure authority is exercised by Joint Staff Foreign Disclosure Officers (FDOs) under the guidance of the Director of the Joint Staff. Management of day-to-day disclosure activity of the Joint Staff foreign disclosure program is the responsibility of the Joint Staff Security Office (JSSO), Foreign Disclosure Division (FDD), and is directed by the Joint Staff FDO. The Joint Staff J2 exercises the foreign disclosure authority of the Director of the DIA for all Joint Staff requests to disclose classified intelligence information. Management of the Joint Staff role on the NDPC and of other international engagement activities is the responsibility of the Joint Staff J-5. The Director for Strategic Plans and Policy, J-5, delegates Joint Staff NDPC representation to J-5, Deputy Director for Partnership Strategy. See Roles and Responsibilities in Enclosure B.

c. Disclosure or denial of Joint Staff CMI will be made only when authorized by officials specifically granted disclosure or denial authority from the Director of the Joint Staff, and after a determination has been made that all of the requirements of reference a and this manual have been met.

d. Disclosure authority delegated pursuant to this regulation pertains only to CMI that meets the limitations and disclosure criteria stipulated in reference a. Reference a, by itself, does not constitute substantive authority to disclose CMI, but rather establishes the eligibility standard to disclose or release such information. Many other considerations must be taken into account before an actual disclosure or release may be made.

e. The Chairman has delegated his authority to disclose CMI to the Commanders of CCMDs through reference c.

APPENDIX A TO ENCLOSURE A

CLASSIFIED MILITARY INFORMATION

1. CMI is military information designated by the Department of Defense (DoD) as requiring protection in the interests of national security. It 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 United States.

2. CMI is arranged into three classifications: TOP SECRET, SECRET, and CONFIDENTIAL, and is grouped into the following eight categories:

a. Category 1 — Organization, Training, and Employment of Military Forces. Military information of a general nature necessary to the organization of military, paramilitary, or irregular forces, to include those tactics, techniques, and tactical doctrine (including military intelligence and counterintelligence doctrine and techniques) necessary to train and employ those forces. This category does not include specific technical data and training needed to operate and maintain individual items of military materiel and munitions.

b. Category 2 — Military Materiel & Munitions. All military materiel, arms, and munitions procured and controlled by the U.S. Government for the equipage, operation, maintenance, and support of its military forces or the military, paramilitary, or irregular forces of its allies. Items developed by U.S. private interests as a result of U.S. Government contracts or derived from technology paid for by the U.S. Government are included within this category. Items on the U.S. Munitions List which may be proposed for sale abroad by U.S. private interests under the International Traffic in Arms Regulations or items specifically covered by other U.S. Government prescribed export control regulations fall within this definition (items under development fall under Category 3). This category also comprises information—to include technical data and training—necessary to operate, maintain, or support specific military materiel, arms, or munitions. It does not include information necessary to produce, coproduce, or in any other way manufacture the item.

c. Category 3 — Applied Research and Development Information and Material. CMI resulting from the extension of fundamental theories, designs, and data from purely theoretical experimental investigations into possible military applications, to include research, the construction and testing of prototypes, and such design changes affecting qualitative performance as may be required during the service life of an item. This also includes engineering data, general operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when materiel has completed operational suitability testing or has for all practical purposes been adopted for military use or production. It includes tactics, techniques,

and tactical doctrine pertaining to specific equipment not yet in production or not yet approved for adoption of U.S. forces. It includes military information, materiel, or munitions under development by U.S. private interests as a result of U.S. Government contracts, or derived from technology paid for by the U.S. Government.

d. Category 4 — Production Information. Designs, drawings, chemical and mathematical equations, specifications, models, manufacturing techniques, software source code, and related information (excluding Category 2 and 3 information) necessary to manufacture or substantially upgrade military materiel and munitions. The following information is furnished to further clarify the definition of Production Information:

(1) Manufacturing Information (more sensitive than Build-to-Print or Assembly information). This includes the know-how, techniques, and processes required to produce or substantially upgrade military materiel and munitions. A manufacturing process or technique is a set of instructions for transforming natural substances into useful materials (metals, plastics, combustibles, explosives, etc.) or for fabricating materials into aerodynamic, mechanical, electronic, hydraulic, or pneumatic systems, subsystems, and components. Software source code, including related documentation that describes software or development know-how for a particular U.S. warfare system that has completed Acquisition Milestone II (Development Approval), or documentation used for production thereof, is considered to be design and manufacturing data and equivalent to Category 4 production information. A manufacturing data package describes how to manufacture, test, and accept the item being produced and what tools and processes are required. Types of manufacturing information include drawings, process sheets, wiring diagrams, instructions, test procedures, and other supporting documentation. Software source code and software documentation that contains or allows access/ insight to classified algorithms or design rationale is considered to be manufacturing information requiring NDPC review and approval. Unclassified software source code and software documentation that is required for minor software maintenance, interface/integration, or to make administrative changes to tables, symbology, markers, or displays will be handled through normal technology transfer channels and does not require NDPC review. Such information will normally be considered for release to foreign customers who possess an indigenous weapon system or verifiable country-unique operation or maintenance requirement the United States is willing to support. Manufacturing information classified solely because of related Category 2 information should be handled as Category 2 information.

(2) Build-to-Print Information (more sensitive than Assembly Information). Assumes the country receiving the information has the capability to replicate an item, sub-system, or component from technical drawings and specifications alone without technical assistance. Release of supporting

documentation (e.g., acceptance criteria, object code software for numerical controlled machines) is permissible. Release of any information which discloses design methodology, engineering analysis, detailed process information, or manufacturing know-how associated with the end item, its subsystems, or components is excluded. Build-to-print information is not considered NDP Category 4 information. Disclosure of Build-to-print information is approved through normal technology transfer channels unless other NDP categories are involved that require NDPC review and approval.

(3) Assembly Information. Normally associated with hardware (parts or kits to be assembled, special tooling or test equipment to accomplish specific tasks) and information that allows assembly and testing of the finished product. Only top level drawings will be released. Detailed assistance is not to be provided, wherein such assistance would provide production or manufacturing techniques. The level and depth of assembly or co-assembly allowed is subject to negotiation and defined in the co-assembly or coproduction agreement. Assembly information is not considered Category 4 production information. Disclosure of assembly information must be approved through normal technology transfer channels unless other NDP categories are involved that require NDPC review and approval.

(4) Effective 6 September 1983, all delegated authority to disclose classified Category 4 production information was canceled. Disclosure programs involving the release of classified Category 4 production information approved prior to this date will remain in effect without an exception to policy provided the programs are not expanded to include significant new technologies. Disclosure programs involving classified Category 4 production information initiated after this date will be submitted to the NDPC for approval as exceptions to policy.

e. Category 5 — Combined Military Operations, Planning, and Readiness. That information necessary to plan, assure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. Includes installations and facilities located within territory under jurisdiction of, or of direct concern to, the recipient foreign government or international organization. This category is limited to that information on installations and facilities—as well as readiness, planning, and operational information—that is necessary to further specific multilateral or bilateral plans and agreements for common defense purposes between the United States and the recipient. It does not include strategic planning and guidance (discussed in Section 1.5.f. of reference a) or North American Defense Information.

f. Category 6 — U.S. Order of Battle. Information pertaining to U.S. forces located within territory that is under the jurisdiction of a recipient government or is otherwise of direct concern to a foreign government or an international

organization. In general, authorization is limited to U.S. order of battle in the recipient countries or in adjacent geographical areas.

g. Category 7 - North American Defense

(1) North American Defense Information is that which concerns plans, programs, projects, operations, and certain specific technical data pertaining to equipment directly related to the defense of North America, especially when it is originated by or under the mission and control of U.S. Northern Command (USNORTHCOM) or North American Aerospace Defense Command (NORAD).

(2) North American Defense Information includes, but is not limited to:

(a) Plans and related documents prepared by United States defense agencies concerning the defense of the United States.

(b) Plans and related documents prepared in combination with the Government of Canada, either bi-nationally (i.e., NORAD) or bilaterally (i.e., between USNORTHCOM and Canadian Joint Operations Command).

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

(d) Information concerning U.S. operational and logistical plans for employment of reserve forces.

(e) Information revealing a vulnerability to the defense of North America, or the vulnerability or official appraisal of the combat readiness of any unit or facility, or the effectiveness of North American defense systems.

h. Category 8 — Military Intelligence. Military intelligence comprises information of a military character pertaining to foreign nations and areas as delimited by the criteria for disclosure of intelligence as stated in Section II of reference a.

ENCLOSURE B

ROLES AND RESPONSIBILITIES

1. The Director, Joint Staff, shall:

a. Act as the Principal Disclosure Authority (PDA) for the Joint Staff.

b. Appoint in writing a Designated Disclosure Authority (DDA) in the Joint Staff Security Office to act as the FDO for the Joint Staff.

c. Provide guidance to the Joint Staff and the Joint Staff FDO on operation of Joint Staff foreign disclosure activities.

2. The Vice Directors of the Joint Staff Directorates shall:

a. Nominate to the Joint Staff FDO in writing primary and alternate Foreign Disclosure Representatives (FDRs) to manage Directorate foreign disclosure actions and coordinate with the Joint Staff FDO.

b. Ensure that all personnel nominated to perform foreign disclosure support functions receive appropriate training as directed by the Joint Staff FDO.

3. The Director for Intelligence, J-2, shall:

a. Appoint a Senior FDO to effectively provide foreign disclosure support to the Joint Staff for Category 8 Military Intelligence information.

b. Provide trained and appointed FDOs from the DIA to support disclosure of Category 8 military intelligence information in execution of Joint Staff and National Military Command Center operations.

4. The Director for Strategic Plans and Policy, J-5, shall:

a. Appoint a representative and alternate to the NDPC to represent the Joint Staff and the Combatant Commanders (CCDRs). If not specifically designated in writing, this authority is delegated to the Deputy Director that represents partnership strategy and policy and associated division chief as the alternate.

b. Advise and assist the Joint Staff FDD and Directorate FDRs on preparation of Requests for Exception to National Disclosure Policy (ENDP) and facilitate submission to the NDPC.

5. The Director, Joint Staff Security Office, shall plan, budget, and provide support for sufficient foreign disclosure and foreign visits personnel to carry out these programs.

6. The Joint Staff Foreign Disclosure Officer shall:

a. Exercise the Chairman's foreign disclosure authority pursuant to appointment by the Director, Joint Staff. Make disclosure decisions in accordance with reference a and this manual.

b. Lead the Joint Staff Security Office, Foreign Disclosure Division (JSSO-FDD).

c. Appoint such other FDOs as are necessary to effectively provide foreign disclosure support to the Joint Staff for Categories 1 – 7 military information.

d. Establish foreign disclosure policy, procedures, and practices for the Joint Staff in compliance with National Disclosure Policy, DoD policies, and Joint Staff Instructions.

e. Coordinate with CCMDs and other agencies outside of the Joint Staff on all matters related to administration of foreign disclosure operations.

f. Maintain the Joint Staff FDO/FDR points of contact list.

g. Ensure initial foreign disclosure training and provide refresher training on an annual basis to all Joint Staff FDOs and FDRs.

h. Advise and assist Joint Staff FDRs.

i. Maintain oversight and accountability of all foreign disclosure decisions made by Joint Staff FDOs for Categories 1 – 7 information.

j. Manage the Joint Staff Foreign Disclosure Management System (FDMS) for tracking and retention of all Joint Staff foreign disclosure actions (both approved and disapproved actions).

k. Establish the Joint Staff Emergency Action Roster to ensure 24-hour availability of FDOs during crisis operations.

l. Manage the Joint Staff Foreign Visits System (FVS) by ensuring that Foreign Visit Requests are received through the DoD FVS, are passed to appropriate Directorate personnel for coordination and approval, receive appropriate foreign disclosure approval, and are routed back through the FVS for return to respective foreign embassies.

m. Submit requests or assist other personnel in preparing requests for ENDPs to the Joint Staff member on the NDPC. Track the requests' progress through the exception process.

n. Ensure that new personnel receive introductory foreign disclosure training as part of their initial indoctrination.

7. The Joint Staff J-2 Foreign Disclosure Officer shall:

a. Make disclosure decisions in accordance with reference a and this manual.

b. Lead the J2 Foreign Disclosure Program (J23-1).

c. Appoint such other FDOs as are necessary to effectively provide foreign disclosure support to the Joint Staff for Category 8 Intelligence information.

d. Ensure initial foreign disclosure training and provide refresher training on an annual basis to all Joint Staff J2 FDOs and FDRs.

e. Advise and assist Joint Staff J2 FDRs.

f. Maintain oversight and accountability of all foreign disclosure decisions made by Joint Staff J2 FDOs.

g. Submit Category 8 intelligence information requests or assist other personnel in preparing requests for ENDPs to the Joint Staff member on the NDPC. Track the request's progress through the exception process.

8. Directorate Foreign Disclosure Representatives shall:

a. Develop and maintain Directorate guidance and administrative procedures concerning management of the Directorate foreign disclosure program. Advise all Directorate personnel on handling potential foreign disclosure issues and direct them to the JS FDO when in need of foreign disclosure assistance.

b. Identify and appoint division-/office-level FDRs.

c. Coordinate foreign disclosure authorizations of Directorate products and ensure that all disclosure actions are properly entered, completed, and recorded in the Joint Staff FDMS.

d. Ensure annual attendance at foreign disclosure refresher training of all Directorate FDRs.

e. Coordinate disclosure requests that include information owned by other Joint Staff offices with the appropriate Office of Primary Responsibility.

f. Coordinate development of requests for ENDP with the Joint Staff FDO.

9. Division/Office Foreign Disclosure Representatives shall:

a. Develop and maintain internal guidance and administrative procedures concerning management of the division/office foreign disclosure program.

b. Ensure compliance with Joint Staff guidance on foreign disclosure and foreign visits.

c. Ensure annual attendance at foreign disclosure refresher training.

d. Coordinate disclosure requests with the Directorate FDR.

10. Joint Staff personnel shall:

a. Abide by the foreign disclosure procedures identified in this manual.

b. When disclosure of CMI to any foreign representative is contemplated or necessary to accomplish an assigned function, request foreign disclosure support from their division/office/Directorate FDRs.

c. Report unauthorized disclosures of CMI to the Joint Staff FDO as soon as possible.

d. If identified as the POC for a foreign visit:

(1) Ensure that Directorate leadership is aware and approves of the proposed visit.

(2) Ensure that classified information to be disclosed is routed for authorization to the Joint Staff FDO via FDMS.

(3) Provide coordination information to the JSSO foreign visits technician.

11. Contact Officers. Joint Staff personnel who are appointed as Contact Officers for Foreign Liaison Officers (FLOs) or Exchange Officers (EXOs) shall:

a. Complete training as directed by the JS FDO for understanding of Contact Officer duties and responsibilities.

b. Become familiar with the Memorandum of Agreement/Arrangement/ Understanding (MOA/U) and the Delegation of Disclosure Authority Letter (DDL) that govern posting of the FLO or EXO.

c. Assist the FLO or EXO in making contact with Joint Staff personnel or other agencies as required to perform assigned duties.

d. Assist Joint Staff or other agency personnel in understanding disclosure rules and limitations for passing CMI to FLOs or EXOs.

e. Ensure that disclosure or release of CMI to FLOs or EXOs is authorized by an FDO.

f. Confirm contact officer appointment and understanding of duties and responsibilities via return letter per DDL Annex B, "Acceptance of Contact Officer Duties."

g. Ensure that the FLO or EXO has signed MOU/A Annex A, certifying that they understand and will comply with administrative and security procedures of the Joint Staff.

12. Commanders of the Combatant Commands shall:

a. Develop procedures for submission, monitoring, and control of visit requests by foreign representatives to their headquarters in accordance with reference c and other applicable DoD guidance.

b. Establish procedures for issue of Invitational Travel Orders (ITOs) in accordance with applicable DoD guidance. Ensure that control of such visits is coordinated with local security and FVS offices well enough in advance to provide necessary information and to preclude embarrassment to the visitor or the U.S. Government.

INTENTIONALLY BLANK

ENCLOSURE C

FOREIGN DISCLOSURE PROCEDURES

1. Introduction. Foreign disclosure processes are tightly controlled throughout the Department of Defense to ensure that such actions complement, are subordinate to, and do not interfere with or contradict the larger U.S. foreign policy effort. Only those individuals who have written authorization may approve disclosures of U.S. CMI. Joint Staff procedures for foreign disclosure will also be tightly controlled through designated and authorized Joint Staff personnel.

2. Requests for Disclosure of CMI

a. All requests for disclosure of CMI in Categories 1 – 7 to foreign governments or international organizations will be referred to the JSSO FDD via the Joint Staff FDMS at: <https://jsportal.osd.smil.mil/JSResources/FDMS_Menu/default.aspx>. Requests for disclosure or release of Category 8 (Military Intelligence) will be directed to the Joint Staff J2 FDO (J23-1). Requestors outside the Joint Staff who are not able to access the FDMS directly may forward their requests to the JSSO FDD via SIPR e-mail or other secure means. Requests to release Joint Staff CUI do not need FDD authorization, but may be referred to office/division/Directorate FDRs for review of accuracy, inadvertent inclusion of classified information, and propriety of release to the intended foreign recipient(s). Such requests may be referred to the JSSO FDD if questions arise.

b. The FDD will analyze the request, contact the requester to obtain any further information that may be required, and may coordinate with any U.S. Government entity outside the Joint Staff that may own any part of the information for authorization to disclose their information. They will consult NDP-1 and other records of action of the NDPC via the DoD National Disclosure Policy System, make a disclosure determination, and provide disclosure authorization back to the requestor.

c. When National Disclosure Policy does not authorize the requested disclosure and the requester wants to pursue an ENDP to allow the disclosure, the FDD will coordinate with the requester and with the J-5 NDPC representative to develop the request for ENDP in accordance with reference b and Enclosure E to this manual. Once the request for ENDP is developed, the Joint Staff NDPC member will coordinate with applicable Joint Staff organizations through the JSAP process, forward the request to the NDPC, and will report the NDPC's action back to the requestor and the FDD.

d. The Joint Staff will maintain records of disclosure authorizations required by reference b in the FDMS. JS FDMS is an automated information

storage and retrieval system with a centralized repository of information pertaining to Joint Staff releases and denials of CMI. FDMS records will be made retrievable through the Joint Staff Documentum system.

3. Use of Foreign Disclosure Management System

a. The Joint Staff FDMS is located at <https://jsportal.osd.smil.mil/JSResources/FDMS_Menu/default.aspx> and on the Joint Staff SIPR portal page, under the "JS Resources" tab or the JS Apps and Tools block.

b. Upon accessing this page, you will see two Joint Staff badges. Click on the one labeled for the category of information you desire to disclose.

c. On the next page you will see a column of tokens linked to various activities. Click on the token labeled for the activity you wish to perform (e.g. "Submit New Document Request").

d. On the next page, answer the questions asked there. Click on the "Attach File" token to upload the basic document with the information you wish to disclose, the source documents from which you built the document to be disclosed, and any other relevant document(s).

e. Go to the bottom of the page and click on the "Save" button.

f. You will receive an e-mail that says that your request has been received.

g. An FDO will be assigned by the JS FDO to handle your request. During analysis, the assigned FDO may contact you with questions. When the FDO has completed analysis, he/she will enter their approval or disapproval into FDMS. You will then receive an e-mail with your disclosure authorization and conditions, or denial.

4. Development and Handling of Requests for Exception to National Disclosure Policy

a. Current foreign disclosure policy may not authorize a contemplated disclosure if the level of classification of the information exceeds the level authorized for the proposed recipient in the disclosure category or if there is another policy statement that places restrictions on the proposed disclosure. One possible course of action is to request an ENDP.

b. Action officers will work with their FDRs using the template at Enclosure E to develop their proposed Request for Exception. They will then send the request to the Joint Staff FDO who will further check existing disclosure policy to ensure that there is no other current policy authorizing the proposed disclosure. If none, the Joint Staff FDO assists the action officer in

sending the request to Joint Staff J5 NDPC representative. The J5 NDPC representative staffs the request via the JSAP system to other Directorates and CCMDs, gathers inputs, prepares the final ENDP package, and transmits it to the NDPC for consideration. Once the NDPC has made their determination and documented it in a Record of Action (RA), they will return it to the Joint Staff and the FDO can authorize disclosure as defined in the RA. See Enclosure E.

c. On 14 February 2017, the Secretary of Defense signed out revisions to reference a codifying the Under Secretary of Defense for Intelligence's (USD(I)) Military Intelligence Disclosure Policy Committee (MIDPC) as the governing committee for disclosure and release of classified military intelligence (Category 8 CMI). As a result, the J2 FDO is the Joint Staff representative to the MIDPC, responsible for advocating CCMD requests for disclosure of Category 8 CMI, with USD(I) as the final adjudicator for Category 8 only requests. This authority follows references d and e.

INTENTIONALLY BLANK

ENCLOSURE D

FOREIGN VISITS PROCEDURES

1. General. Most visits of representatives of foreign governments to the Joint Staff will be coordinated by their Washington, D.C., embassies through the DoD FVS. DoD guidance is contained in reference f. FVS is a computerized system managed by DIA and hosted on the Defense Technology Security Administration's Security Policy Automated Network (SPAN). Embassy staffs enter information for each visit request to a DoD office or DoD contractor facility into FVS at their respective embassies. FVS forwards the visit request to DIA for routing to the visited facility.

2. Foreign Visit Request Handling

a. FVS technicians in the JSSO FDD receive FVS Visit Requests to the Joint Staff and route them to the points of contact (POCs) in the appropriate Directorates or offices to be visited via Joint Staff unclassified network e-mail. The e-mail asks the POC whether the visit is authorized and at what disclosure level discussions or presentations will be conducted. The POC coordinates as needed inside the office and responds to the FDD with authorization or denial, and recommended security classification level if appropriate.

b. The FDD also makes a disclosure decision for the visit as confirmed by the POC and provides that information back to the POC and the FVS technician in the FDD. The FVS technician completes the Joint Staff response in FVS and releases the case back to DIA for response back to the embassy.

c. POCs for visits wherein classified information will be discussed must forward proposed briefing slides or other documentation to the FDD through FDMS for disclosure authorization in sufficient time prior to the visit to ensure that disclosure is in compliance with NDP.

3. Visits for Training. Security Cooperation Offices (SCOs) at U.S. embassies in foreign countries may invite members of foreign military services to the United States to attend training under International Military Education and Training or other programs. Such activities are done in accordance with reference g, but no visit request is submitted through FVS. To effect these invitations, SCOs issue ITOs to each foreign trainee as discussed in reference g. When properly filled out, the ITO contains security clearance information on the individual trainee in the same way that security clearance information is passed in the FVS. Visits to Joint Staff offices for training purposes where the trainee has been issued an ITO will be handled in accordance with reference h.

4. Foreign Liaison Officers and Exchange Officers. Enclosure B, paragraph 10, lists duties and responsibilities of contact officers for FLOs and EXOs. Embassies send extended visit requests for their FLOs and EXOs through the FVS prior to their arrival. No FLO or EXO may be posted to the Joint Staff or communicate with the Joint Staff until an MOU/A exists, a DDL has been written, and a visit request received and approved. References i and j contain Joint Staff policy and procedures for hosting long-term foreign visitors and shall be consulted when such a posting is contemplated and initiated.

5. Visits and Assignments of Foreign Representatives to the Headquarters of Combatant Commands. Visits and assignments of foreign representatives to the headquarters of CCMDs shall be controlled and monitored in accordance with the following:

a. In accordance with reference f, requests from foreign representatives to visit the headquarters of CCMDs within the United States shall be submitted through the sponsoring government's embassy in Washington, D.C., or by the sponsoring international organization using the FVS and International Visit Procedures (IVP). Commanders of U.S. European Command (USEUCOM) and U.S. Africa Command (USAFRICOM) shall develop procedures to be used by foreign governments and international organizations to request similar visits to their headquarters. These procedures shall include provisions to document visit requests and staffing for approval or denial, as well as foreign disclosure authorizations for CMI, if any, to be disclosed during the visit.

b. CCMDs will follow all appropriate procedures in the Military Departments' and DIA's guidebooks for foreign visitors, liaison officers, or attachés. If the requesting agency does not have access to SPAN then the respective CCMD FDO will submit a request for visit authorization on behalf of the requesting foreign national.

c. If a CCDR extends a visit invitation to a foreign representative, has issued ITOs and is paying for the visit, and no classified information will be discussed, the visit request need not be submitted through the foreign national's embassy. However, if the visit will involve classified information, a request must be submitted through the requesting government's embassy in Washington, D.C., or as directed in procedures established by USEUCOM and USAFRICOM.

d. Foreign visitor clearance to an overseas component of a Military Service will be the responsibility of the parent Service.

e. If the visit of a foreign representative includes disclosure of classified information, provisions of the National Disclosure Policy will apply. When requirements for delegated disclosure authority exceed those in reference a, authorization for disclosure must be obtained from the NDPC through a request for ENDP developed and submitted in coordination with the JS FDO and Strategic Plans and Policy Division, Joint Staff J-5.

f. When a CCDR deems a proposed visit of a foreign representative to be politically sensitive, advance coordination with the Chairman of the Joint Chiefs of Staff must be sought prior to issuing an invitation.

g. Foreign visitor clearance to overseas subcomponents and task forces of CCMDs will be the responsibility of the CCDR. Procedures will be established to ensure that contacts with foreign representatives by DoD officials that involve access to U.S. classified information conform with:

(1) National Disclosure Policy.

(2) Security and foreign policy interests of the United States.

(3) Reference c.

h. Although foreign visit requests are managed, processed, and recorded by DIA or the Services, the CCDRs retain responsibility for the visit, disclosures during the visit, security, and protocol.

i. Clearances noting access to Sensitive Compartmented Information must be vetted through the appropriate national level authority for that organization; e.g., the Central Intelligence Agency for general intelligence and human intelligence, the National Security Agency for signals intelligence and communications intelligence, etc.

INTENTIONALLY BLANK

ENCLOSURE E

REQUESTS FOR EXCEPTION TO NATIONAL DISCLOSURE POLICY

1. Requests for ENDPs are submitted to the NDPC via respective NDPC members for vote. The ENDP request should provide essential information necessary for voting members to make an informed decision on granting authority to the requesting member to disclose CMI to foreign governments via national representatives. NDP-1 must be reviewed when considering disclosures of CMI.

2. An ENDP request should contain, at a minimum, the following areas of discussion:

a. Purpose of the Exception. The purpose states the authorization the Joint Staff will gain from approval of the request in general terms. The purpose should list the classification level(s) and associated categories of CMI, proposed recipient government(s) or organizations, and the reason(s) for the release.

b. Requirement for an Exception. The requirement is a simple statement that identifies why an exception is necessary. This is typically stated in terms such as "an exception to policy is required because the information proposed for disclosure exceeds the classification level delegated to the Joint Staff in… [Annex A of NDP-1]."

c. Background and Description. Self-explanatory.

d. Consistency with U.S. Policy and Benefits to the U.S. Government. The objectives of this section are to illustrate how disclosure is consistent with U.S. policy and to assess the level of benefit the U.S. Government achieves through sharing CMI with the recipient foreign government or international organization. U.S. policy in this term comprises foreign policy, national security objectives, and military and security objectives. Additionally, the request must show that disclosure will result in a clearly defined advantage to the United States.

e. Security Protection. This section must provide an assessment that the foreign recipient will afford CMI substantially the same degree of security protection given to it by the United States. The intent of a foreign government to protect U.S. CMI is established in part by the negotiation of a General Security of Information Agreement or other similar security arrangement. Guidance in determining a foreign government's capability to protect U.S. CMI may be determined by an embassy security assessment, CIA risk assessment,

and/or an NDPC Security Survey Report. FDOs can determine whether such agreements exist.

f. Conditions and Limitations. Self-explanatory. This section should provide the necessary detailed conditions and limitations used to mitigate the risks associated with disclosure to a foreign recipient so as to maintain a clearly defined advantage [benefit] to the United States. While typically technical in nature, this section is also the place to include the proposal on whether disclosure will be limited to oral and/or visual means or will include release of some physical item such as a briefing or pamphlet. Justification must be provided to show that the information proposed for disclosure is limited to information necessary to the purpose for which the disclosure is made. Additionally, any instructions on how release will be presented to avoid creating any false impressions of U.S. Government readiness to make available classified military material, technology, or information should be included.

g. Supplemental information. This section provides additional information such as the nature of the request (one-time or continuing), the required suspense for an NDPC decision, Joint Staff points of contact, and any necessary supporting documents or amplifying remarks.

h. On 14 February 2017, the Secretary of Defense signed out revisions to NDP-1, codifying USD(I)'s MIDPC as the governing Committee for disclosure and release of classified military intelligence (Category 8 CMI). As a result, J2 FDO is the Joint Staff representative to the MIDPC, responsible for advocating CCMD requests for disclosure of Category 8 CMI, with USD(I) as the final adjudicator for Category 8 only requests. This authority follows references d and e.

ENCLOSURE F

REFERENCES

a. National Disclosure Policy - 1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations"

b. DoD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

c. CJCSI 5221.01 series, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations"

d. JSM 5100.01 series, 21 February 2014, "Organizations and Functions of the Joint Staff," page F-6

e. MOA 017-002, December 2002, "MOA between the DIA and the JS on the Provision of Intelligence Support"

f. DoD Directive 5230.20, 20 June 2005, "Visits and Assignments of Foreign Nationals"

g. Defense Security Cooperation Agency, DSCA 5105.38-M, "Security Assistance Management Manual (SAMM)"

h. CJCSI 2211.01 series, "Visits by Students or Staff Members of Foreign National or International Defense Colleges"

i. JSI 2220.01 series, "Joint Staff Foreign Engagement and Hosting of Long-Term Foreign Visitors Validation Policy"

j. JSM 2225.01 series, "Hosting Long-Term Foreign Visitors to The Joint Staff"

k. National Security Decision Memorandum 119

PART II - RELATED

l. Arms Export Control Act (22 U.S.C. 2751)

m. Export Administration Act (50 App. U.S.C. 2401 et seq.)

n. Executive Order (EO) 13526

o. DoD 5200.01-M, 24 February 2012, “DOD Information Security Program, Vols. I - IV”

p. CJCSM 5220.01 series, “Joint Staff Information and Physical Security Programs Manual”

q. DoD Directive 4500.54, 28 December 2009, “DoD Foreign Clearance Program”

r. DoD 5400.7-R, 4 September 1997, “DoD Freedom of Information Act Program”

s. DoD Directive 5230.25, 6 November 1994, “Withholding of Unclassified Technical Data from Public Disclosure”

t. DoD Instruction 5230.24, 23 August 2012, “Distributions Statements on Technical Documents”

u. DoD 5220.22-M, 8 February 2006, “National Industrial Security Program Operating Manual (NISPOM)”

APPENDIX A TO ENCLOSURE F

ADDITIONAL POLICY INFORMATION

1. National Disclosure Policy. NDP-1 (reference a) implements NSDM-119 (reference k). The NDPC formulates foreign disclosure policy and procedures, and considers requests for exceptions to the policy. The NDPC is guided by the policy and procedures contained in NDP-1, which has been approved by the Secretaries of State and Energy and the Director of Central Intelligence, and issued by the Secretary of Defense. NDP-1 is a controlled document that may be accessed only by PDAs or DDAs, the Joint Staff NDPC representatives, and Joint Staff Foreign Disclosure Officers. Other Joint Staff personnel will receive disclosure guidance as described in Enclosures B and C. Only the Secretary of Defense, Deputy Secretary of Defense, and the chairperson of the NDPC are authorized to approve an ENDP. NDP-1 provides the following:

a. Disclosure Criteria and Limitations. NDP-1 requires that specified criteria and limitations be satisfied in order to disclose CMI to representatives of foreign governments or international organizations.

b. Categories of CMI and Delegation of Disclosure Authority Charts. Annex A to NDP-1 contains charts that identify the eight categories of information that constitute CMI (see Appendix A to Enclosure A). The charts provide guidance on the maximum classification level within each category of CMI that may be disclosed to the foreign governments and international organizations specified in the charts. If a disclosure must be denied because the NDP-1 criteria and conditions cannot be met, an ENDP may be sought. The content of the charts is classified and may not be shared with any foreign person, entity, government, or international organization.

c. NDPC Policy Statements. Annexes B and C to NDP-1 contain NDPC Policy Statements that provide specific policy guidance related to certain countries or international organizations and to certain weapons systems, technologies, or other matters of concern.

d. False Impressions. Pursuant to Part II paragraph 2 of reference (a), Joint Staff personnel must scrupulously avoid any action that creates a false impression that the United States is willing to enter into any arrangement with a foreign government that will involve eventual disclosure of CMI. Therefore, before a JS Directorate enters into an initiative with a foreign government that will entail eventual disclosure of any CMI, the Directorate shall obtain disclosure authority sufficient to provide all of the information of the type and at the classification level that is known or anticipated for the life of the program or initiative.

e. Reporting of Compromises

(1) The U.S. Government is obligated by international agreements that are concluded pursuant to NDP-1 to report to the originating government the loss or compromise of classified FGI.

(2) NOTE: The NDP-1 promulgates the national policy and procedures and provides criteria, limitations, and terms of reference for making decisions on disclosure of any CMI. It does not provide the authority to execute a sale or other transfer of articles, services, or technical data to a foreign government or international organization.

2. DoD Directive 5230.11. This directive (reference b) implements NDP-1 within the Department of Defense. It delegates disclosure authority to the heads of certain DoD Components, including the Chairman of the Joint Chiefs of Staff. It requires that each DoD Component with delegated disclosure authority appoint a PDA to oversee the Component's foreign disclosure program. The Directive permits the DoD Components to re-delegate disclosure authority to subordinate commands, agencies, and staff elements as necessary to ensure efficient operations, provided that a DDA is appointed at each such command, agency, or staff element to oversee foreign disclosure activities. The Directive requires the DoD components to record their decisions on disclosures of CMI.

3. DoD Directive 5230.20. This directive (reference (f)) establishes DoD policies and procedures for visits or assignments of foreign representatives to DoD Components and DoD cleared contractor facilities. It establishes the DoD IVP, the DoD FLO Program, the DoD Personnel Exchange Program, and the conditions for assignment of Cooperative Program Personnel. It requires the DoD Components to establish information access and physical procedures for controlling access by foreign nationals to classified information and programs.

4. Arms Export Control Act and Export Administration Act. The Arms Export Control Act (AECA) (reference (l)) governs exports of classified and unclassified defense articles and services and related technical data to foreign countries and international organizations. It is the principal statute that governs international commercial and government sales, co-production arrangements, loans, leases and grants of defense articles, as well as DoD participation in cooperative arms programs. The AECA is the legal basis for security arrangements for most DoD international programs. It stipulates that recipient countries and international organizations that receive U.S. defense articles and services must agree to specified conditions on retransfer, end-use, and protection of the articles and related technical data. The Export Administration Act (reference (m)) governs export of unclassified items and technical data that have civil application as well as those items and technical data that have both a civil and military application ("dual-use" items).

5. Executive Order (EO) 13526. EO 13526 (reference (n)) establishes the U .S. National Security Information Program and governs classification, declassification, downgrading, and safeguarding of classified national security information. The EO states that access to classified information must be in support of a lawful and authorized governmental purpose, and that the ability of a potential recipient to provide protection must be verified prior to a release of the information. The EO further specifies that classified information cannot be shared with a third party without the consent of the originator. In addition, U.S. Government departments and agencies are required to protect FGI, classified or unclassified, that is provided in confidence.

6. NSDM-119. NSDM-119 (reference (k)) establishes the basic U.S. policy for disclosure of CMI to foreign governments and international organizations and assigns oversight responsibility jointly to the Secretaries of State and Defense. The Secretaries of State and Defense are required, in coordination with the Secretary of Energy, the Director of Central Intelligence, and the heads of other departments and agencies, as appropriate, to establish procedures and an interagency mechanism to implement the national policy.

7. DoD 5200.01-M, DoD Information Security Program. DoD 5200.01-M (reference (o)) implements reference (m) by establishing DoD policy and procedures for classification, safeguarding, accessing, transmitting, and declassifying U.S. CMI and CUI. It describes Original Classification Authority (OCA) and rules for exercising that authority. OCA is important in the foreign disclosure process in that the ultimate authorization and control of disclosure or release of CMI and associated CUI often rests with the OCA who originally classified it. 5200.01-M also describes DoD policy and procedures for protecting unclassified information that has not been approved for release pursuant to a request under the Freedom of Information Act (FOIA). It defines the term “For Official Use Only” (FOUO) and prescribes rules for its use. It also establishes the requirement for review of all unclassified FOUO information prior its disclosure or release to any foreign representative. Reference (p) implements reference (o) for the Joint Staff.

8. DoD Directive 4500.54. This directive (reference (q)) establishes DoD policies and procedures for temporary travel by DoD personnel overseas. It requires, among other things, that the DoD Components establish procedures to ensure that requests for travel authorization include a statement certifying that the appropriate disclosure authorization has been approved. If the traveler is to carry classified information, compliance with the required security procedures also must be certified.

9. DoD 5400.7-R, DoD Freedom of Information Act Program. Generally, the U.S. public is entitled to have access to federal agency records unless the information in the records is protected from public disclosure by one of nine

exemptions. Pursuant to reference (r), information that is determined to be exempt from disclosure by a DoD Component normally is to be marked "For Official Use Only" or "FOUO" if it is not classified. Some information that is determined to be exempt from public disclosure will bear other markings, such as "Unclassified Controlled Nuclear Information," which also is marked "UCNI," and medical and personnel files, which are marked with privacy statements. Because unclassified information that qualifies under FOIA for withholding from public disclosure is of such sensitivity that it is not available to the U.S. public, it must undergo a review to determine if it may be authorized for release to foreign governments and international organizations and their representatives, but this is not a foreign disclosure review.

10. DoD Directive 5230.25. DoD Directive 5230.25 (reference (s)) implements Public Law 98-94 (10 U.S.C. 130), which authorizes the Secretary of Defense to withhold from public disclosure certain export-controlled technical data with military or space application. The legislation includes a specific definition of technical data which must be used in determining whether data is actually exempt from public disclosure. This legislation, however, does not apply to scientific, educational, or other data not directly and significantly related to design, production, or utilization in industrial processes. The directive addresses export control of U.S. data.

11. DoD Instruction 5230.24. DoD Instruction 5230.24, Distributions Statements on Technical Documents, (reference (t)) lists the distribution statements to be attached to unclassified documents containing technical data as defined in 10 U.S.C. 130. These distribution statements are to be used in marking technical data only. The distribution statements tell holders of the documents who may receive copies of them and the technical data contained therein. These distribution statements are meant for U.S. holders only and do not in themselves address disclosure to foreign governments.

12. DoD 5220.22 -M National Industrial Security Program Operating Manual (NISPOM). This manual (reference (u)) provides guidance to DoD personnel and to contractors on security of activities under contracts with the U.S. Government. It provides some guidance on contractor performance under U.S. activities with foreign governments or international organizations, but should not be used as a primary reference in carrying out foreign disclosure or foreign visits activities

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk (*) *have definitions in PART II*

CCMD	Combatant Command
CMI	Classified Military Information
CUI	Controlled Unclassified Information
DDA	Designated Disclosure Authority
DDL	Delegation of Disclosure Authority Letter
DIA	Defense Intelligence Agency
ENDP	Exception to National Disclosure Policy
FDD	Foreign Disclosure Division
FDO	Foreign Disclosure Officer
FVS	Foreign Visits System
JDir	Joint Staff Directorate
JSSO	Joint Staff Security Office
NDPC	National Disclosure Policy Committee
PDA	Principal Disclosure Authority
RA	Record of Action (of the NDPC)
SPAN	Security Policy Automated Network

INTENTIONALLY BLANK

PART II-DEFINITIONS

Controlled Unclassified Information (CUI). Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country that has not been authorized by the U.S. Government for release to anyone without a need to know. It includes U.S. information that is determined to be exempt from public disclosure as described in references (m) and (n) or that is subject to export controls of the International Traffic in Arms Regulations or the Export Administration Regulations. (Source: DoDD 5200.01-M, Vol. IV).

Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate Designated Disclosure Authority (i.e., Joint Staff Foreign Disclosure Officer) explaining classification levels, categories, scope, and limitations of information under a DoD Component's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities. (Source: DoDD 5230.11).

Designated Disclosure Authority (DDA). An official designated by the DoD Component's Principal Disclosure Authority who has been delegated authority in accordance with reference (b) to control disclosures by subordinate commands or staff elements of CMI to foreign governments, their national representatives, and to international organizations. (Source: DoDD 5230.11).

Disclosure. The approved conveyance of CMI via oral and/ or visual transmission of information through approved channels to authorized representatives of foreign governments or international organizations. Authorization of disclosure of information does not necessarily include authorization to release information in any physical format. (Source: NDP-1).

Eligibility. An individual country's or international organization's prescribed potential to receive U.S. CMI within a certain NDP-1 category of information. Granting eligibility is not automatic, but subject to final approval by the Department of State and Central Intelligence Agency via Security Surveys and Risks Assessments. (Source: NDP-1).

Exception to National Disclosure Policy (ENDP). Exceptions to the National Disclosure Policy will be requested by members of the NDPC to the Chairman, NDPC. The Joint Staff NDPC representative is in the J-5/ Partnership and Strategy Division. (Source: NDP-1).

False Impression. It is the policy of the United States to avoid creating false impressions of its readiness to make available classified military materiel, technology, or information. Proposals to foreign governments and international organizations which result in US or combined initial planning, and which will lead to eventual disclosure of classified military materiel, technology, or information, including intelligence threat data or countermeasures information, must be authorized in advance by designated disclosure officials in the departments and agencies originating the information, or by the National Disclosure Policy Committee. (Source: NDP-1)

Foreign Disclosure Management System (FDMS). A Joint Staff automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release CMI and technology to other nations and international organizations.

Foreign Disclosure Officer (FDO). An individual designated in writing with the authority and responsibility to oversee and control coordination of specific disclosure of CMI.

Foreign Disclosure Representative (FDR). An individual who assists directorate action officers in obtaining foreign disclosure authorization for proposed disclosures of specific CMI that is originated or owned within the FDR's specific division or office. FDRs are designated in writing by either the Joint Staff FDO or their Directorate FDR.

Foreign Government Information. Classified information received from allies or other coalition partners. It will be protected at the equivalent U.S. classification level and only released to third parties based on guidance received from the originating country. (Source: DoDD 5200.01-M, Vol. I).

Foreign National. A person who is not a citizen or national of the United States. (Source: DoDD 5230.20).

Foreign Representative. Any person, regardless of citizenship, who represents a foreign government or international organization to the U.S. Government or its contractors. For example, a U.S. Citizen assigned to NATO may represent NATO to the U.S. Government, but is considered and must be treated as a foreign representative despite his/ her U.S. citizenship.

International Organization. An entity established by recognized governments pursuant to an international agreement that, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies. (Source: DoDD 5230.11).

Military Information. Information under the control or jurisdiction of the Department of Defense, its departments, or agencies, or of primary interest to them. Military information may be embodied in equipment or may be written, oral, or other form. Military information may be classified or unclassified. (Source: DoDD 5200.01-M, Vol. I).

National Disclosure Policy (NDP-1). NDP-1 promulgates national disclosure policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance required by U.S. departments and agencies having occasion to release CMI to foreign governments and international organizations. In addition, it establishes and provides for management of interagency mechanisms and procedures required for effective implementation of the policy. (Source: NDP-1).
National Security Information. Information that has been determined, pursuant to Executive Order 13526, or any predecessor order, to require protection against unauthorized disclosure.

Release. The approved conveyance of CMI in physical form through approved channels to authorized representatives of foreign governments or international organizations. "Release" refers to the transmission of CMI in any physical format, to include documents, films, recordings, tapes, e-mails, and web-based products on authorized networks. (Source: DoDD 5230.20)

INTENTIONALLY BLANK