DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

MCO 5510.20C
PP&O (PL)
18 Nov 2020

MARINE CORPS ORDER 5510.20C

From: Commandant of the Marine Corps
To: Distribution List

Subj: DISCLOSURE OF MILITARY INFORMATION TO FOREIGN GOVERNMENTS AND INTERESTS

Ref: See Enclosure (1)

Encl: (1) References
(2) Foreign Disclosure Definitions
(3) Foreign Disclosure Policy
(4) Example of Request for Disclosure Authorization
(5) NDP-1 Categories of Classified Military Information
(6) NDP-1 Disclosure Criteria, Conditions, and Limitations
(7) USMC International Visits Program Guidance and Procedures
(8) Additional Guidance Regarding Extended Foreign Visits
(9) Examples of Contact Officer Documents
(10) Foreign Disclosure Officer Approval Marking

1. Situation. This Order establishes United States Marine Corps (USMC) policy, procedures, authority, and responsibilities for the disclosure of U.S. Classified Military Information (CMI) and Controlled Unclassified Information (CUI) to foreign governments and international organizations in accordance with references (a) through (ag). It also establishes policies, procedures, and authorities within the USMC for processing visit requests from foreign governments and international organizations, to include guidance for liaison between representatives of the USMC and foreign governments and interests, and implements references (a) through (d).

a. This Order applies to:

(1) All foreign disclosures of CMI and CUI defined in enclosure (2). Disclosures of military intelligence information must also comply with reference (f).

(2) Any foreign nationals or foreign entities representing their parent governments or international organizations on official business visiting or assigned to USMC activities or cleared contractor facilities or visiting at any location in the United States or abroad and discussing official business.

b. This Order does not apply to:

(1) The disclosure of CMI and CUI to foreign nationals who are employed by Department of Defense (DoD) components or DoD contractors per reference (t). Such persons do not represent nor are they sponsored by a

government and, therefore, are not foreign representatives to whom the disclosure of CMI and CUI may be made under this Order.

(2) Information that is releasable to the Public Domain in accordance with reference (p).

(3) Visits of foreign nationals that fall within the exemptions outlined in enclosure (7).

(4) Other exemptions listed in references (a) and (d).

2. Cancellation MCO 5510.20B, MARADMIN 110/19.

3. Mission The USMC fully supports national disclosure policy and the International Visits Program (IVP) in accordance with references (a) through (d), (o), and (t), and provides appropriate safeguards for the protection of our national security interests while building and enhancing relationships with allies and other friendly nations. Foreign disclosure policy and processes must be followed whenever CMI and CUI may be shared with foreign governments or international organizations, and information will be shared only when reviewed and approved by a Foreign Disclosure Officer (FDO), in accordance with this Order and the references.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) The USMC supports the DoD mission and U.S. foreign policy by cooperating with our allies to the fullest extent possible in the development of mutual defense against potential adversaries, while providing safeguards in the protection of our national security interests in accordance with reference (j).

(b) The disclosure of CMI and CUI to our military allies is a significant aspect of this cooperation. The net benefit to the United States and the need to protect and conserve our military information must be measured on a case-by-case basis.

(c) No staff agency, command, or activity within the USMC will disclose or direct the disclosure of CMI or CUI except as approved or authorized by an FDO in accordance with this Order.

(d) The decision to grant access to CMI and CUI during visits and assignments of foreign nationals shall be consistent with the national security and foreign policy interests of the United States and the government-to-government principle per references (a) through (d) and (t). Only foreign nationals who represent or are officially sponsored by their governments or international organizations, i.e., official visitors, may have access to such information and only when approved by an FDO and in accordance with the IVP and guidance outlined in enclosure (7).

(2) Concept of Operations

(a) In accordance with reference (i) and to ensure proper coordination and control of foreign disclosure within the USMC, DC PP&O is

designated as the disclosure authority for NDP-1 Categories 1 through 7, and DC I as the disclosure authority for NDP-1 Category 8, as outlined in enclosure (5).

(b) Disclosure authority includes responsibility for ensuring compliance with the provisions of any treaty, agreement, statute, executive order, directive, or instruction involving the disclosure of military information to foreign governments and international organizations.

(c) Requests for disclosure shall be processed and coordinated in accordance with references (a) through (d), (f), (t), and this Order.

(d) CMI and CUI originated by other U.S. Government agencies or military services may be disclosed only with the approval of the appropriate disclosure authority from the originating agency or military service.

b. Re-delegation of Disclosure Authority. Reference (i) grants the authority to re-delegate disclosure authority to subordinate commands. In order to decentralize disclosure decisions, accurately safeguard CMI and CUI, and streamline the disclosure process, disclosure authority is re-delegated as follows:

(1) DC PP&O may re-delegate disclosure authority for appropriate NDP-1 Categories 1 through 7 to the commanding generals of Marine Component and supporting establishment commands. DC PP&O may also re-delegate disclosure authority for NDP-1 Categories 1-7 to other deputy commandants at their request.

(2) DC I may re-delegate authority for NDP-1 Category 8 information to USMC directors, commanders, or officials when such authority is determined to be mission essential or in the best interest of the U.S. Government.

(3) Marine component commanders and supporting establishment commanding generals may further re-delegate disclosure authority to subordinate general officer commanders. Commanders may also re-delegate to commands headed by Colonels (or Colonel equivalent). O-6 level commands who, due to their mission, are involved in extensive international engagements such as exercises, operations, training, and foreign visits may hold disclosure authority. Examples of such commands are: Marine Expeditionary Units, Special-Purpose Marine Air-Ground Task Forces, Marine Expeditionary Force (MEF) Information Groups, USMC Intelligence Schools, USMC Security Cooperation Group, and Marine Aviation Weapons and Tactics Squadron One. Commanding generals or commanders with disclosure authority, or their FDOs, may appoint FDRs at all subordinate commands that deal with foreign entities, and those FDRs will coordinate CUI and CMI decisions with FDOs at the parent commands, unless the FDR has written authority to make CUI decisions, in which case, the FDR does not need to coordinate with the FDO on CUI decisions.

(4) The location of the primary command FDO within the command structure is ultimately at the discretion of the commanding general/commanding officer based upon local foreign disclosure requirements. If it is determined that the primary FDO billet will not be a Special Staff position, the placement of the billet within the command structure should not restrict or delay information regarding foreign disclosure issues from reaching the planners and the Commander in a timely manner.

(5) FDRs may be appointed to assist FDOs or placed in subordinate commands that have only occasional contact with foreign personnel or international organizations. Commanders with disclosure authority or their designated FDOs may grant disclosure authority to approve CUI to government civilian or military FDRs. FDRs granted CUI disclosure authority must be appointed in writing and their appointment letters must specify exactly what types of CUI and what NDP-1 Categories of information they are authorized to approve. FDRs who have not been granted disclosure authority in writing are not authorized to make foreign disclosure decisions on behalf of a command, but should process and coordinate foreign disclosure requests for CUI and CMI and make recommendations to FDOs. FDRs who are contractors shall not have authority to approve CUI. Under no circumstances will an FDR, government or contractor, be granted authority to approve CMI requests. There is no rank requirement for FDRs, but they must hold security clearances at least commensurate with the level of information that they are required to review.

(6) FDOs and FDRs must complete mandatory training as prescribed by DC PP&O (PL), DC I (DIRINT), and their local command policy, as applicable. Commands shall not appoint FDOs or FDRs until they have a certificate of completion from the two-day Marine Corps Foreign Disclosure Officer Certification Course provided by a Mobile Training Team led by DC PP&O (PL). The following additional prerequisites will be used in selecting Category 8, Military Intelligence FDOs:

(a) Only Uniformed personnel within the 02XX, or 26XX military occupational specialties (E-6 and/or O-3 and above) and/or government civilian employees in the GG/GS-0132 series with a paygrade of GG/GS 11 or above may be appointed as Category 8 FDOs. Exception can be granted to non-0132 civilians with DIRINT approval.

(b) Recipients granted this authority must be U.S. citizens and must have been the subject of a favorably adjudicated T5 or T5R to the Top Secret/Sensitive Compartmented Information (TS/SCI) level completed within the last five years or as required by DoD policy.

(c) FDOs who will approve disclosure/release of intelligence information must complete additional Defense Intelligence Agency (DIA) training and eligibility for appointment must be confirmed by DC I (DIRINT) in accordance with references (ac) and (ad). Contact DC PP&O (PL) or DC I (DIRINT), as appropriate, to arrange for training.

(d) When deciding who will be appointed as a unit’s FDO, effort should be made to choose someone who currently holds a T5 or T5R clearance. Assignment as a unit’s FDO normally is not sufficient justification for investigation/SCI eligibility determination. The Category 8 FDO appointee shall have Joint Worldwide Intelligence Communications System (JWICS) access.

(7) Upon completion of the training requirements and an appointment letter from their commander, FDOs may request access to NDP-1 from DC PP&O (PL). Only FDOs will be authorized access to NDP-1, in accordance with reference (b).

(8) All commands, regardless of location, that have disclosure authority shall develop and implement local IVP policy and shall establish accounts in the DoD FVS and the DoD FVS-CM to support the USMC IVP. All commands will ensure that information to be disclosed during foreign visits is properly reviewed, and appropriately marked to indicate approval by an

FDO. In addition, there must be verification that the foreign visitor has the proper security assurance from his/her embassy to receive the information planned for disclosure during the visit, and that all disclosures are properly documented in the FDMS. Comprehensive guidance regarding the IVP, including FVS and FVS-CM, can be found in enclosure (7), and references (t) and (y). The USMC FDO approval marking can be found in enclosure (10).

(9) Commands shall include foreign disclosure awareness/ indoctrination as part of their overall training plans and conduct command foreign disclosure awareness training at least annually. Two online options for local training are on MarineNet and MILSUITE. Users can access the MarineNet course through the following URL: https://www.marinenet.usmc.mil/MarineNet/Courses/CourseDetails.aspx/fdo1intro01. MILSUITE training can be accessed through the following URL: https://www.MILSUITE.mil/university/usmcforeigndisclosure-class/, then find the course under the "Training for all Marines" section in the microlearning library. Both MarineNet and MILSUITE offer a certificate of completion which should be provided to the FDO/FDR to track command training. Local briefs provided by the FDO are also an option, and a roster of attendees can serve as proof of training completion.

(10) Disclosures and denials of CMI and CUI shall be documented in the FDMS, and disclosure records of CMI must be maintained in FDMS in accordance with references (m) and (ae). Commands can get guidance for local installation of FDMS from the HQMC PL Foreign Disclosure SharePoint site at: https://eis.usmc.mil/sites/hqmcppo/PL/PLA/PLFD. Local information technology (IT) personnel should be able to assist with installation.

c. Responsibilities

(1) Deputy Commandant for Plans, Policies, and Operations (DC PP&O)

(a) Act as Executive Agent for general foreign disclosure matters and this Order.

(b) Re-delegate foreign disclosure authority for NDP-1 Categories 1-7 to USMC component commands, commanding generals of supporting establishment commands, and appropriate HQMC staff agencies.

(c) Assist commands in developing and implementing local foreign disclosure policy, as needed.

(d) Appoint at least one FDO within DC PP&O (PL) to oversee the USMC Foreign Disclosure Program and provide USMC foreign disclosure policy guidance regarding NDP-1 Categories 1-7.

(e) Coordinate requests for foreign disclosure that do not fall under the authority of another FDO with HQMC staff agencies, USMC commands, other services, contractor facilities, and stakeholders, as appropriate. Render decisions on appropriate CUI and CMI requests in accordance with references (a) through (c) and (t).

(f) Write DDLs and oversee all disclosure policy pertaining to Personnel Exchange Program (PEP) and Foreign Liaison Officer (FLO) assignments in accordance with references (a) through (d) and (t).

(g) Act as the OPR for all extended FVRs, described in enclosures (6) and (7), and review, coordinate, and provide appropriate decisions regarding such visits. Support DC I (DIRINT) on FVS matters, as required.

(h) DC PP&O International Affairs Branch (PLU) desk officers should coordinate with affected commands and contractor facilities regarding feasibility of operational support for foreign visits, as required.

(i) DC PP&O (PL) FDOs will conduct foreign disclosure reviews for one time and recurring foreign visits to HQMC staff agencies that do not have disclosure authority and to commands that do not fall under the authority of another FDO, as required.

(j) Ensure extended visits by FLOs and PEPs are under the auspices of a specific agreement or annex to a previously concluded umbrella agreement i.e., Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or a Foreign Military Sales (FMS) Letter of Offer and Acceptance (LOA), in accordance with references (d) and (t).

(k) Ensure a specific billet description for a PEP has been established by the host command or its higher headquarters. Ensure a general billet description for a FLO has been provided by the host command or its higher headquarters in coordination with the FLO's embassy. Complete a disclosure review for all extended visits and ensure a DDL has been written and briefed to the host command prior to approval of an extended FVR. See enclosures (6), (7), and (8) for guidance and appropriate documentation regarding extended foreign visits.

(l) Assign/provide augment personnel to the IGMC inspection team on matters related to IGMC Inspection Checklist 5510.2 and the general subject of foreign disclosure. Provide reports to IGMC as appropriate after all inspections. Train all FDOs as inspectors and inspector trainers so they can properly conduct command unit inspections. As custodian of functional area Checklist 5510.2, ensure currency and accuracy of the checklist.

(m) Provide training to FDOs and FDRs through site assist visits, disseminating information regarding Mobile Training Team (MTT) courses, online MarineNet, microlearning training, or any other means, as needed. Train select, experienced FDOs from various USMC activities as instructors and develop, train, and oversee MTTs to conduct FDO/FDR certification training at USMC activities, as needed.

(n) Coordinate all requests for Exceptions to National Disclosure Policy (ENDP) and other issues that require development of new Department of the Navy (DON) policy with Navy International Programs Office (NIPO) per reference (t).

(o) Act as the USMC general member on the Technology Transfer Security Assistance Review Board (TTSARB) and coordinate TTSARB documents to appropriate USMC activities to determine: Political-military implications, consistencies with previous disclosure decisions, balance between risk of sharing technology with benefits of engagement and building partnership capacity, interoperability considerations, and affected Marine component commander perspective.

(p) Submit requests for screening and vetting of all extended foreign visitors to the Marine Corps Intelligence Activity (MCIA) via the DON

Identification and Screening Information System (DONISIS) per enclosure (7). In order to expedite screening and vetting, all available information on foreign visitors should be provided. Marine Corps organizations hosting extended foreign visitors shall resubmit extended visit personnel for screening and vetting on the anniversary of the initial screening each year for the duration of their assignments.

(q) In coordination with MCIA, develop a process for automating biographic information input to the FVS into DONISIS to expedite the screening and vetting of official foreign visitors. Information shared between PP&O and MCIA will be conducted pursuant to law, policy, and regulation governing intelligence information collection and sharing.

(2) Deputy Commandant for Aviation (DC AVN)

(a) Unless foreign disclosure authority is delegated to DC AVN, designate one or more individuals to coordinate with DC PP&O (PL) FDOs and provide guidance and subject matter expertise regarding aviation-related foreign disclosure and technology transfer matters.

(b) In coordination with DC PP&O (PL), review all aviation-related extended FVRs and, in coordination with DC I (DIRINT), review one-time and recurring FVRs for all visits hosted by DC AVN.

(c) DC AVN may authorize the embarkation of foreign nationals in USMC aircraft for the purpose of practical demonstration and orientation when foreign disclosure guidance has been provided by DC PP&O PL. Foreign military personnel must possess proper base/installation visitation authorization pursuant to established policies and procedures. Basic policies concerning embarkations and disclosure of CMI and CUI in connection with such embarkations is contained in references (a) through (f), (h), (t), and (u) through (w).

(d) DC AVN is the approval authority for foreign passengers to receive orientation/indoctrination flights in high performance jet, tilt-rotor, and AH-1 aircraft, following foreign disclosure guidance provided by DC PP&O PL. Foreign disclosure guidance will cover personnel occupying a crew seat position, riding in the back of an aircraft, riding in aircraft with personal oxygen systems, and riding in an aircraft during shipboard catapult launches or arrested landings, in accordance with references (t) and (w).

(e) DC AVN delegates authorities relating to orientation/indoctrination flights within CONUS for foreign passengers/ nationals (military and civilian) aboard USMC cargo/ transport aircraft subject to the limitations outlined in reference (w), and in accordance with foreign disclosure guidance.

(3) Deputy Commandant for Installations and Logistics (DC I&L).

(a) Unless disclosure authority is delegated to DC I&L, designate one or more individuals to coordinate with DC PP&O (PL) FDOs and provide disclosure authorization and guidance regarding installations and logistics matters.

(b) Establish policy to support the IVP for security assurances to allow foreign nationals access to USMC installations.

(c) Ensure all USMC installations establish FVS accounts to support and facilitate foreign visits to each USMC installation.

(d) Ensure all USMC installations establish counterintelligence and force protection measures, to include the screening and vetting of foreign visitors, to assist with protecting DoD personnel, family members, resources, facilities, and critical infrastructure against foreign intelligence threats.

(4) Deputy Commandant for Information (DC I)

(a) Has the authority to delegate foreign disclosure authority for NDP-1 Category 8 information to USMC commands or officials when DC I determines either of the following:

1. Such authority is mission essential.

2. Such authority is in the best interest of the U.S. Government.

(b) May delegate disclosure authority for NDP-1 Category 8, Intelligence information, to DC I (DIRINT).

(c) Appoint one or more FDOs within the DC I Department or at subordinate activities to provide USMC foreign disclosure policy guidance regarding NDP-1 Category 8.

(d) Ensure FDOs coordinate with the Defense Intelligence Agency (DIA), combatant commands, DON commands and other appropriate stakeholders, and render decisions regarding requests for disclosure and release of Category 8 CUI and CMI, in accordance with references (a) through (d), (f), (g) and (t).

(e) Ensure FDOs process and coordinate with the DIA and the National Security Agency (NSA) all intelligence-related international agreements in accordance with reference (c).

(f) Coordinate, either directly or through FDOs in DC PP&O (PL), and provide disclosure authorization guidance and limitations for all Category 8 CMI for foreign exchange and foreign liaison assignments in accordance with references (a) through (d), (f), (g) and (t).

(g) Act as the Executive Agent for the USMC IVP.

(h) Maintain a Foreign Visits System (FVS) account with headquarters-level permissions and authorities, and receive, review, and coordinate the staffing and processing of all one-time and recurring FVRs, as outlined in enclosure (7) Support DC PP&O (PL) on FVS matters, as required.

(i) Conduct liaison with national representative FLOs (Foreign Attachés).

(j) Implement counterintelligence and force protection measures, to include Technical Surveillance Countermeasure (TSCM) support, CI awareness and reporting (CIAR) briefings, CI debriefings, and CI screening and vetting of foreign visitors to assist with protecting DoD personnel, family members,

resources, facilities, and critical infrastructure against foreign intelligence threats. MCIA is the Service Intelligence Center responsible for providing intelligence support to service-retained entities. Those entities with their own organic intelligence or counterintelligence elements may conduct their own intelligence screening in coordination with MCIA. Refer to enclosure (7) for more guidance on screening and vetting of foreign visitors.

(k) Coordinate with DC PP&O (PL), as appropriate, regarding disclosure decisions and provide guidance and subject matter expertise regarding foreign disclosure and technology transfer for all command, control, communications, and computer-related matters.

(l) Coordinate with DC PP&O (PL) regarding TTSARBs or ENDPs with an intelligence interest.

(5) Deputy Commandant, for Combat Development and Integration (CD&I)

(a) Appoint in writing by name at least one primary FDO and one alternate FDO or an FDR to oversee CD&I's Foreign Disclosure Program, as defined in enclosure (2), and provide a copy of appointment letters to DC PP&O (PL) and/or DC I (DIRINT), as appropriate.

(b) Re-delegate disclosure authority to subordinate divisions and ensure FDOs are appointed, as appropriate, to oversee foreign disclosure programs.

(c) Develop and implement local foreign disclosure and foreign visits policy in accordance with references (a) through (d) and (t).

(6) Assistant Deputy Commandant for Plans, Policies, & Operations (Security) (PS). Coordinate with DC PP&O (PL) and commands hosting FLO, PEP, or other foreign exchange personnel, to ensure proper security policies are in place which prevent inadvertent disclosure or uncontrolled access to spaces where CMI and/or CUI is stored or discussed.

(7) Inspector General of the Marine Corps (IGMC). Coordinate, conduct, and evaluate inspections of Fleet Marine Forces (FMF) and supporting establishment commands, units and activities, including operational forces assigned to the unified and specified commands, to ensure compliance with foreign disclosure and foreign visits policy outlined on IG Checklist 5510.2 in accordance with references (a) through (d), and this Order.

(8) Director, Communication Directorate. Coordinate visits by foreign journalists and freelance writers with the Department of State (Undersecretary for Public Diplomacy and Public Affairs) for U.S. Government clearance and approval in accordance with reference (s), and notify MCIA Marine Corps Counterintelligence Coordinating Authority for CI Screening. These visits are not official visits and so will not be processed via the FVS and will be limited to unclassified information approved for release to the public domain.

(9) Commanding General, Training and Education Command (TECOM)

(a) Appoint in writing by name at least one primary FDO and one alternate FDO or an FDR to oversee TECOM's Foreign Disclosure Program, as

defined in enclosure (2), and provide a copy of appointment letters to DC PP&O (PL) and/or flash DC I (DURIENT), as appropriate.

(b) Re-delegate disclosure authority to subordinate divisions and ensure FDOs are appointed, as appropriate, to oversee foreign disclosure programs.

(c) Provide at least one FDO with at least two years of foreign disclosure experience to serve as an instructor on the Marine Corps Foreign Disclosure Officer Certification Course Mobile Training Team (MTT) which provides a two-day course at commands throughout the USMC several times a year.

(d) In coordination with DC PP&O (PL), local FDOs, and TECOM, ensure that appropriate foreign disclosure approval is in place for all USMC schools and courses that are attended by foreign nationals.

(e) Develop and implement local foreign disclosure and foreign visits policy in accordance with references (a) through (d) and (t).

(10) Commander, Marine Corps Systems Command (MARCORSYSCOM)

(a) In coordination with DC PP&O (PL) and in accordance with references (e), (h), (k), (n), and (q), oversee foreign disclosure for ground systems and equipment.

(b) Appoint one or more FDOs to oversee the MARCORSYSCOM Foreign Disclosure Program.

(c) Develop and implement local foreign disclosure and foreign visits policy in accordance with references (a) through (d) and (t).

(d) Provide foreign disclosure guidance to commands involved in foreign visits, exercises, or operations with foreign countries when U.S. ground equipment will be used or displayed.

(e) Provide foreign disclosure guidance to TECOM and its formal schools when training of foreign students involves use or display of U.S. ground equipment.

(f) In coordination with DC PP&O (PL) and Navy IPO, and in accordance with references (n) and (t), oversee the USMC export license process.

(g) Provide general officer level approval for TTSARB cases for ground equipment submitted to Navy International Programs Office and coordinate with DC PP&O (PL) on all TTSARB cases with a MARCORSYSCOM interest.

(h) Provide at least one FDO with at least two years of foreign disclosure experience to serve as an instructor on the USMC Foreign Disclosure Officer Certification Course MTT which provides a two-day course at commands throughout the USMC several times a year.

(11) Commanders/Commanding Generals

(a) Marine commanders with disclosure authority shall appoint at least one primary FDO and one alternate FDO or an FDR, as defined in enclosure (2), by name and in writing, and provide a copy of the appointment letters to DC PP&O (PL) and/or DC I (DIRINT), as appropriate. The FDO may be assigned full-time, part-time, or as a collateral duty, depending on the needs of the command, and must be a civilian employee GS-11 equivalent or above, a military officer O-3 or above, or senior enlisted E-6 or above, with sufficient authority and staff to manage the command's program. Primary command FDOs must be U.S. citizens and must have been the subject of a favorably adjudicated Tier 5 (T5) or T5R completed within the last five years or as required by DoD policy. Individuals with current T5 investigations, or equivalent investigations, should be designated as the organization primary FDOs whenever possible. Alternate FDOs/FDRs must have security clearances at least commensurate with the level of information that they will be required to review, but only one FDO per organization is required to have a current T5. Category 8, Military Intelligence, FDOs must have further qualifications identified in Paragraph 4 b (8) below. The Billet Identification Code (BIC) for the FDO billets with T5 or T5R will be coded in the Total Force System.

(b) Ensure USMC foreign disclosure and release actions are conducted in accordance with applicable directives, regulations, instructions, and orders and maintain all foreign disclosure decision records in the FDMS.

(c) When a command FDO/FDR and alternate are absent, submit foreign disclosure requests, via FDMS or by using the form provided in enclosure (4), to the next higher command with an FDO or to DC PP&O (PL), as appropriate, for disclosure or release of CUI and CMI in Categories 1 through 7, and to DC I (DIRINT) for CUI or CMI in Category 8.

(d) At commands with FLO, PEP, or other exchange personnel assigned, appoint a Contact Officer and an alternate Contact Officer, by name and in writing, as described in enclosure (8). Ensure the Contact Officers have satisfied training requirements by completing the MarineNet Foreign Disclosure Contact Officer Course mandated by DC PP&O, and any other requirements dictated by local policy, and adhere to assigned responsibilities.

(e) Maintain a Foreign Visits System (FVS) account, and ensure that the command reviews and confirms feasibility of support for all foreign visits affecting the command, as described in enclosure (7), and makes timely approval/disapproval decisions within FVS. All FVRs must be coordinated for foreign disclosure by an FDO and for counterintelligence concerns by the appropriate authority before a proposed command visit is to take place.

(f) Ensure the FDO or another person in the command, as appropriate, has access to an FVS account and the FVS-CM, and adheres to the guidelines outlined in reference (d), enclosures (5) and (6), and local policy.

(g) Establish and maintain, at the lowest supporting level, local standard operating procedures, directives and guidance regarding foreign disclosure and foreign visits in accordance with references (a) through (d), (t) and this Order.

(h) In coordination with MCIA and DC PP&O (PS), implement counterintelligence and force protections measures, to include the screening and vetting of foreign visitors, to assist with protecting DoD personnel, family members, resources, facilities, and critical infrastructure against foreign intelligence threats.

(i) FDOs, and those who manage the Foreign Visits System (FVS) and the Foreign Visits System-Confirmation Module (FVS-CM) who are not FDOs, shall familiarize themselves with the Inspector General of the Marine Corps (IGMC) functional area checklist 5510.2 for foreign disclosure and be prepared to assist command Inspectors General with inspections of subordinate units when tasked. The most current functional area checklist can be found on the IGMC site: https://www.hqmc.marines.mil/igmc/Units/Inspections-Division/Functional-Area-Checklists-FACs/.

d. Coordinating Instructions

(1) DC PP&O (PL), MARCORSYSCOM, and the FMF coordinate all Exceptions to National Disclosure Policy (ENDP) and TTSARBs with Navy IPO in accordance with this order, references (a) through (c), (t), and (x).

(2) Requests for disclosure review of CMI and CUI will be forwarded by the respective USMC command to the first FDO in the chain of command. Regardless of whether or not a command has original classification authority, the FDO must obtain originator consent and coordinate reviews with all interested stakeholders in accordance with reference (t). USMC commands and HQMC staff agencies that do not have disclosure authority should forward foreign disclosure requests to the next FDO in the chain of command using the FDMS. FDMS requests shall include supporting rationale to include the benefit to the United States in sharing the information. After the appropriate FDO makes a decision, an email will be generated by the FDMS and sent to the requestor advising that the product has been reviewed and that the final decision and instructions are available on the FDMS. When use of the FDMS is not available or practical, requests for foreign disclosure review may be sent to the FDO via email, and the FDO will then enter the disclosure request into the FDMS so that the decision will be documented. Requests that do not provide sufficient detail on which to base a decision will be denied or returned for further justification.

e. International Agreements. The Secretary of the Navy (SECNAV) has delegated to the Commandant of the Marine Corps (CMC) the authority to negotiate and conclude certain international agreements, to include personnel exchange agreements. All commands engaging in activities that assist in the creation of new international agreements, in accordance with reference (l), shall coordinate with DC PP&O (PLU).

f. Meetings, Symposia, and Conferences

(1) Foreign Participation. Foreign nationals may participate in meetings, symposia, conferences, or other such activities when their participation is in accordance with this Order, U.S. export control policies, the appropriate FDO has approved any CMI or CUI that will be disclosed to foreign attendees, the foreign attendees actively participate in the proceedings, and there is reciprocity for the U.S. Government and industry representatives.

(2) Disclosure Levels. The classification levels and categories of information authorized for disclosure vary among nations. USMC components shall limit the level of classified information to be disclosed at meetings attended by foreign representatives to the lowest level that is common to all nations represented in accordance with reference (b).

g. Sales, Leases, Loans, or Grants of Classified Items. All requests for disclosure or commercial export of any CUI or CMI relating to sales, leases, loans, grants, or foreign test and evaluation of military ground equipment shall be coordinated with MARCORSYSCOM International Programs (IP).

h. Requests for Classified Documents

(1) Disclosure Review. Official requests for classified documents from foreign representatives shall be forwarded to the appropriate FDOs at the originating USMC components for review and decisions, or to DC PP&O (PL) if no other FDO can be identified.

(2) Reference Lists and Bibliographic Material. To avoid false impressions of United States readiness to make available classified military materiel, technology or information, and to avoid proliferation of requests for CMI or CUI that are not releasable to the requestor, USMC components shall not:

(a) Reference documents that have not been approved by an FDO, unless they are releasable to the public domain.

(b) Approve release of documents that have reference lists or bibliographies. (Identify the requestor's specific requirements and provide only the U.S. information that satisfies that requirement and which is determined to be releasable.)

i. Reporting Compromises of U.S. CMI Furnished to Foreign Governments. In accordance with reference (a), USMC activities having knowledge of compromises of U.S. classified information to foreign persons shall promptly inform the originating USMC component and DC PP&O (PL). The originating USMC component shall conduct a Preliminary Inquiry (PI) and damage assessment and forward the results to DC PP&O (PS) and (PL). DC PP&O (PL) and (PS) shall forward PIs and damage assessments to MCIA's Marine Corps Counterintelligence Coordinating Authority for possible screening and vetting when foreign persons are named who may have initially received compromised information. DC PP&O (PL) shall report such disclosures to the National Disclosure Policy Committee via Navy IPO, if required.

j. Foreign Access to Information When Participating in U.S. Procurement Programs. Refer all such requests for foreign access to information when participating in U.S. procurement programs to MARCORSYSCOM (IP) for processing ground equipment and to DC PP&O (PL) for processing aviation platforms or systems, in accordance with this Order and references (h) and (k).

5. Administration and Logistics

a. Records Management. Records created as a result of this directive shall be managed according to National Archives and Records Administration (NARA)-approved dispositions per SECNAV M-5210.1 to ensure proper maintenance, use, accessibility and preservation, regardless of format or

medium. Records disposition schedules are located on the Department of Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to MCO 5210.11F for Marine Corps records management policy and procedures.

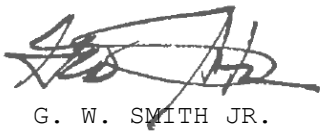
b. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The Department of the Navy (DON) recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a) and implemented per SECNAVINST 5211.5F.

c. Recommendations. Any recommendations concerning the content of this order may be sent to Plans, Policies, and Operations (PP&O), PL Division, Foreign Disclosure (FD) office via the proper chain of command.

6. Command and Signal

a. Command. This Order is applicable to the USMC Total Force.

b. Signal. This Order is effective the date signed.



G. W. SMITH JR.
Deputy Commandant for
Plans, Policies, and Operations

DISTRIBUTION: PCN 10208490800

References

(a) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," dated June 16, 1992
(b) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations Disclosure Policy-1 (NDP-1), with Changes, dated Feb 14, 2017 (NOTAL)
(c) SECNAVINST 5510.34B
(d) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," dated June 22, 2005
(e) 22 U.S.C. 2751
(f) DoD Directive C-5230.23, "Intelligence Disclosure Policy," dated November 18, 1983 (NOTAL)
(g) Defense Intelligence Agency (DIA) Instruction 2000.001, "International Military Intelligence Relationships," dated February 12, 2004
(h) Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 27
(i) Director, Navy International Programs Office Delegation of Disclosure Authority Letter to the Commandant of the Marine Corps, dated April 12, 2005 (NOTAL)
(j) MCO 5710.6D
(k) 22 CFR 120-130, International Traffic in Arms Regulations (ITAR)
(l) DoD Instruction 5530.03, "International Agreements," Dec 4, 2019
(m) SECNAV M-5210.1
(n) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," CH-1 dated July 31, 2017
(o) E.O. 13526
(p) DoD Directive 5400.07, "DoD Freedom of Information Act Program," dated April 5, 2019
(q) 15 CFR 730-799, Export Administration Regulations (EAR)
(r) 10 U.S.C. 2350a
(s) SECNAVINST 5720.44C CH-2
(t) SECNAV M-5510.1
(u) DoD Instruction 4515.13 CH-5, "Air Transportation Eligibility," October 23, 2020
(v) OPNAVINST 3710.7V
(w) MCO 3710.8
(x) SECNAVINST 4900.46D
(y) FVS-CM Directive MEMO mandatory FVS-CM DoDD 5230-20
(z) DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) dated 18 May 2016
(aa) U.S./Canada Joint Certification Program (JCP) dated December 1996
(ab) DoD Manual 5200.01 Volume 3 CH-3, "DoD Information Security Program: Protection of Classified Information," July 28, 2020
(ac) Memo I-00/012863-IS to NDP-1
(ad) Memo 23435-2697 to the Director, DIA
(ae) MCO 5210.11F
(af) 5 U.S.C. 552a
(ag) SECNAVINST 5211.5F

Foreign Disclosure Definitions

1. Classified Military Information (CMI). Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL. CMI may be in oral, visual, or material form and has been divided into eight categories. (See enclosure (5) of this order for a listing of the eight categories.) Military Information may also be embodied in equipment, software, firmware, databases, imagery, or other forms. (SECNAV M-5510.1)

2. Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material. (SECNAV M-5510.1)

3. Compromise. An unauthorized disclosure of classified information. (SECNAV M-5510.1)

4. Contact Officer. A DON official designated in writing to oversee and control all contacts, requests for information, consultations, access, and other activities of foreign nationals who are assigned to, or are visiting, a DON Component or subordinate organization. For Defense Personnel Exchange Program (DPEP) assignments, the host supervisor may be the Contact Officer. (SECNAV M-5510.1)

5. Controlled Unclassified Information (CUI). Unclassified information to which access or distribution controls have been applied in accordance with national laws, policies, and regulations. CUI is a term used to collectively describe unclassified information that has been determined to be exempt from mandatory disclosure to the public pursuant to the Freedom of Information Act (5 U.S.C. 552) and in accordance with references (p) and (t) of this Order, or that is subject to U.S. export controls in accordance with the ITAR and EAR. *Within the DoD most of this information is marked "For Official Use Only" or "FOUO"; however, there are exceptions to the FOUO marking. Unclassified Controlled Nuclear Information (UCNI) is marked as such; personnel and medical files are marked with privacy statements; contractor information marked "PROPRIETARY" or "Business-Sensitive" will be handled as FOUO when provided to DoD/DON; and there are special distribution and export control warning notices that are applied by DON Components to DON documents that contain critical technology with a military or space application.* (SECNAV M-5510.1)

6. Cooperative Program Personnel. Foreign government personnel, assigned to a multinational program office that is hosted by a DON Component in accordance with the terms of a cooperative program international agreement, who report and take direction from a DON-appointed program manager (or program manager equivalent) for the purpose of carrying out the multinational project or program. Foreign government representatives described in such agreements as liaison officers or observers are not considered Cooperative Program Personnel and are treated as FLOs. (SECNAV M-5510.1)

7. Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on

behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities. (DoDD 5240.02)

8. Defense Articles. Weapons, weapon systems, munitions, aircraft, boats, or other implements of war; property, installations, material, equipment, or goods used for the purposes of furnishing military assistance or making military sales; any machinery, facility, tool, material, supply, or other items necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any other defense article or component or part of any articles listed above. Defense articles do not include merchant vessels, major combatant vessels, or as defined by the Atomic Energy Act of 1954, as amended (Title 42 U.S.C. 2011), source material, by-product material, special nuclear material, production facilities, utilization facilities, or atomic weapons or articles involving Restricted Data. (SECNAV M-5510.1)

9. Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate designated disclosure authority 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. Under no circumstances may the contents of DDLs be disclosed or acknowledged to foreign representatives. (DoDD 5230.11)

10. Designated Disclosure Authority (DDA). An official at a DON organization (e.g., command, agency, staff element) who has been granted a Delegation of Disclosure Authority Letter (DDL) by Navy IPO and that is responsible for controlling disclosures of CMI and CUI at that organization. (SECNAV M-5510.1)

11. Documentary Information. Any information, which is recorded on paper, film, transparency, electronic medium, or any other medium. This includes, but is not limited to printed publications, reports, correspondence, maps, audiotapes, email, spreadsheets, databases and graphical slides, technical drawings, software code, and information embodied in hardware. (SECNAV M-5510.1)

12. Export License. The authorization issued by the State Department, Office of Defense Trade Controls, or by the Department of Commerce, Bureau of Industry and Security, which permits the export of ITAR or EAR controlled articles, technical data, or services. (SECNAV M-5510.1)

13. Foreign Disclosure. The disclosure of CMI or CUI to an authorized representative of a foreign government or international organization. (The transfer or disclosure of CMI or CUI to a foreign national who is an authorized employee of the U.S. Government or a U.S. contractor is not a "foreign disclosure," since the disclosure is not made to the person's government. Access for contractor employed foreign nationals is subject to the provisions of the Arms Export Control Act or Export Administration Act and the National Industrial Security Program Operating Manual. Access for foreign nationals part of DON organizations will be in compliance with DoD Regulation 5200.2-R and DoD Regulation 5200.1-R implemented by SECNAVINST 5510.36 and SECNAVINST 5510.30A.) (SECNAV M-5510.1)

14. Foreign Disclosure Officer (FDO). An official at a DON organization (e.g., command, agency, staff element) who has been granted authority to control disclosures of CMI and CUI at that organization. This disclosure

authority must be granted by the issuance of a Delegation of Disclosure Authority Letter (DDL). The delegation authority may be issued by Navy IPO, or the Commander/Commanding Officer upon whom the DDL is issued, or a senior FDO with re-delegation authority. (Note: The Commandant of the Marine Corps has a DDL from Navy IPO giving USMC full disclosure authority for USMC information and authority to re-delegate.) (SECNAV M-5510.1)

15. Foreign Disclosure Representative (FDR). DON officials who are appointed for the coordination of foreign disclosure reviews and to facilitate a complete and timely response to foreign requests for CMI or CUI representing the consolidated organization position. (SECNAV M-5510.1)

16. Foreign Government Information (FGI). Information provided to the United States by a foreign government or governments, an international organization, or any element thereof, with the expectation that the information, the source of the information, or both are to be held in confidence; produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or information received and treated as FGI under the terms of Executive Order 12958. (SECNAV M-5510.1)

17. Foreign Liaison Officer (FLO). A foreign government military member or civilian employee authorized by his or her government and 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 that government. There are three types of FLOs:

a. Security Assistance. A foreign government representative who is assigned to a DoD/DON Component or contractor facility in accordance with a requirement that is described in a Foreign Military Sales (FMS) Letter of Offer and Acceptance (LOA).

b. Operational. A foreign government representative who is assigned to a DoD/DON Component in accordance with a documented requirement to coordinate operational matters, such as combined planning or training and education.

c. National Representative. A foreign government representative who is assigned to his or her national embassy or delegation in the United States (e.g., an attaché), to conduct liaison activities with the DoD and the DoD Components. (SECNAV M-5510.1)

18. Foreign National. A person who is not a citizen or national of the United States. (SECNAV M-5510.1)

19. Foreign Representative. A person, regardless of citizenship, who represents a foreign interest in his or her dealings with the U.S. Government, or a person who is officially sponsored by a foreign government or international organization. A U.S. national shall not be treated as a foreign person except when acting as a foreign representative. (SECNAV M-5510.1)

20. Foreign Visit. Any contact by a foreign representative with a DoD/DON organization or contractor facility. Such visits are of two types, based on sponsorship:

a. Official Foreign Visit. Contact by foreign representatives under the sponsorship of their government or an international organization with a DoD component or DoD contractor facility. Only official visitors may have access to classified or Controlled Unclassified Information.

b. Unofficial Foreign Visit. Contact by foreign nationals with a DoD/DON command or activity for unofficial purposes, such as courtesy calls and general visits to commands or events that are open to the public, and without sponsorship of their government. Such visitors shall have access only to information that has been approved for public disclosure. Foreign nationals not sponsored by their government, visiting under the terms of a DoD/DON contract are not considered foreign visitors and will be cleared in accordance with the National Industrial Security Program Operating Manual Section 5, paragraph 10-507. (SECNAV M-5510.1)

21. Government-to-Government Channels. The principle that classified information and materiel will be transferred by government officials through official government channels (e.g., military postal service, diplomatic courier) or through other channels expressly agreed upon in writing by the governments involved. In either case, the information or material may be transferred only to a person specifically designated in writing by the foreign government as its designated government representative for that purpose. (SECNAV M-5510.1)

22. International Organization. An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies. This typically refers to the North Atlantic Treaty Organization (NATO), or one of its elements. (SECNAV M-5510.1)

23. Naval Nuclear Propulsion Information (NNPI). Information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities. Information concerning equipment, components, or technology which are applicable to both Naval nuclear and conventional propulsion plants is not considered to be NNPI when used in reference to conventional applications only, provided no association with naval nuclear propulsion can be directly identified from the information in question. In cases where an association with naval nuclear propulsion can be directly identified from the information in question, designation as NNPI is mandatory. (SECNAV M-5510.1)

24. Oral/Visual Disclosure. To brief orally, expose to view, or permit use under U.S. supervision to permit the transfer of knowledge or information, but not to physically transfer documents, material, or equipment to a foreign government or its representatives. Note taking is not authorized under this disclosure method since notes connote a physical or permanent transfer. (SECNAV M-5510.1)

25. Personnel Exchange Program (PEP). A program under which military and civilian personnel of the Department of Defense and military and civilian personnel of the defense ministries and/or military services of foreign governments, in accordance with the terms of an international agreement, occupy positions with and perform functions for a host organization to

promote greater understanding, standardization, and interoperability. (SECNAV M-5510.1)

26. Principal Disclosure Authority (PDA). The PDA oversees compliance with SECNAV M-5510.1 within the DON and is the only DON official other than the Secretary or Under Secretary of the Navy who is authorized to deal directly with the Secretary or Under Secretary of Defense regarding such matters as DON requests for exceptions to the National Disclosure Policy. The PDA for the DON is the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)). Navy IPO has been designated by ASN (RD&A) to act on his behalf as the PDA for the Navy. (SECNAV M-5510.1)

27. Release. Release authority is inherent in a disclosure authorization unless it is specifically limited to oral/visual only. This term is superseded in this order under the term "disclosure." In practice, a release occurs when any information that is recorded on paper, film, transparency, electronic medium, or any other medium, is physically or electronically transferred to a foreign government or its representatives, or a recipient of a licensed export. It includes, but is not limited to, the transfer of printed publications, reports, correspondence, maps, audiotapes, email, spreadsheets, databases and graphical slides, technical drawings, software code, and information embodied in hardware. (SECNAV M-5510.1)

28. Security Assurance. Written confirmation requested by and exchanged between governments of the security clearance level and eligibility of their employees or national contractors to assume custody of classified information on behalf of the recipient government. There are two additional types of security assurances:

a. Facility Security Clearance Assurance (FSCA). A certification provided by a government on a contractor facility under its territorial jurisdiction which indicates that the facility is cleared to a specific security level and has suitable security safeguards in place at the specified level to safeguard classified information.

b. Personnel Security Clearance Assurance (PSCA). This pertains to an individual who is to be employed by a government or its contractors and requires a personnel security clearance (i.e., a Limited Access Authorization in the U.S.). It is a statement provided by the security authorities of the individual's country of citizenship concerning the individual's eligibility for a personnel security clearance at a level equivalent to the level specified by the requesting (host) government. (See also DoD 5200.2-R) (SECNAV M-5510.1)

29. Security Policy Automation Network (SPAN). A wide area computer network sponsored by the Defense Technology Security Administration consisting of a DoD-wide Secret classified network and a separately supported unclassified network that supports communications and coordination among DoD activities on foreign disclosure, export control, and international arms control and cooperation. (SECNAV M-5510.1)

30. Sensitive Compartmented Information (SCI). Information and material that require special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established. (SECNAV M-5510.1)

31. Technical Data. Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, manuals, and documentation.

a. Classified information relating to defense articles and services.

b. Information covered by an invention secrecy order.

c. Software directly related to defense articles.

d. This definition does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. (SECNAV M-5510.1)

32. Technology. Information, including scientific information, which is necessary for the research, development, design, and manufacture of end products. (SECNAV M-5510.1)

33. Third Party Transfer. The retransfer of a defense article by a foreign government or foreign entity, that was originally provided the article by the U.S. government or a U.S. entity, to any entity not an officer, agent, or employee of that government or entity. The USG generally limits the definition of "agent" to mean freight forwarders. Third party transfer includes the retransfer of a defense article by a foreign government or foreign entity, that was originally provided the article by the U.S. government or a U.S. entity, to a foreign government or foreign entity of the same origin but who is not an agent/employee of the original foreign government or entity. (SECNAV M-5510.1)

34. U.S. Citizen. For the purposes of this manual, a person either naturalized as a U.S. citizen in accordance with U.S. Immigration and Naturalization laws and regulations or a person born in one of the following locations: any of the 50 states of the U.S., the District of Columbia, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands, Panama Canal Zone (if the father and/or mother was/were, or is/was a citizen of the U.S.), the Federated States of Micronesia, or the Republic of the Marshall Islands. (SECNAV M-5510.1)

35. U.S. National. A citizen of the U.S. or a person who, though not a citizen of the U.S., owes permanent allegiance to the U.S., e.g., a lawful permanent resident of the U.S. Categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. are listed in 8 U.S.C. §1101(a) and 8 U.S.C. §1401, subsection (a) paragraphs (1) through (7). Legal counsel should be consulted when doubt exists as to whether or not a person can qualify as a national of the U.S. A U.S. national shall not be treated as a foreign person except when acting as a foreign representative. (SECNAV M-5510.1)

Foreign Disclosure Policy

1. Only a USMC military or civilian official who has been appointed in writing as a Foreign Disclosure Officer (FDO) may authorize foreign disclosure of CMI or CUI. FDOs may re-delegate authority to disclose certain CUI to U.S. Government Foreign Disclosure Representatives (FDR) on a case-by-case basis. Contractors may be appointed as FDRs but shall not hold disclosure authority for CUI or CMI. All disclosures will be for a lawful and authorized purpose in accordance with references (a) through (c) and (t). The following guidance must be met:

a. The official representative of a USMC component who submits information for foreign disclosure review must use the Foreign Disclosure Management System (FDMS). If FDMS is unavailable, requestors may email disclosure requests to FDOs or FDRs using the sample letter provided in enclosure (4) with the material to be reviewed. The FDO can upload the request and the final decision into FDMS when the system is available to document the decision. Requestors must obtain the written consent of the relevant official having original classification authority or ownership of the requested information before submitting the request for disclosure. If the requestor cannot obtain originator consent in writing, he/she must provide the FDO with a point of contact who can give originator consent to disclose the information to a foreign entity.

b. The level of classified information to be disclosed does not exceed the classification level delegated in reference (b), unless a National Disclosure Policy Committee (NDPC) or a Military Intelligence Disclosure Policy Committee (MIDPC) Record of Action authorizes a higher level of disclosure authority. See appendix (j) of reference (t) for instructions regarding completion of a request for Exception to National Disclosure Policy (ENDP). See enclosure (5) for a listing of NDP-1 categories of information.

c. Disclosure criteria, conditions, and limitations in reference (b) and enclosure (6) shall be satisfied.

2. CMI shall not be disclosed to foreign nationals until the appropriate FDO receives security assurance from the recipient foreign government or international organization, normally through an approved Foreign Visit Request (FVR), for the individuals who are to receive the information. Additionally, the host commands shall ensure that the security clearance level of the foreign visitor, as specified by the foreign embassy in the FVR or other assurances consistent with reference (ab), is at least at the classification level of the information that is approved for disclosure during the visit.

3. CMI and CUI in document, material, or any other form approved for foreign disclosure and release shall be transferred to the intended foreign recipient only through official government-to-government channels or through other channels that have been agreed to in writing by the responsible security officials of the governments involved pursuant to references (a), (c) and (t). Hard copy documents should not be released to foreign personnel.

4. Per reference (b), it is the policy of the United States to avoid creating a false impression of its readiness to make available classified military materiel, technology, or information. Therefore, initial planning with foreign governments and international organizations concerning programs that might involve the eventual disclosure of CMI may be conducted only if it

is explicitly understood and acknowledged that no United States commitment to furnish such classified information is intended or implied until disclosure has been approved by the appropriate disclosure authority.

5. All official visits by foreign representatives must be controlled as outlined in enclosure (7).

6. Disclosure planning shall include the following:

a. An FDO must be involved from the outset regarding any plans for operations, exercises, training, acquisition programs, or other possible foreign involvement to ensure that all requirements can be supported within the construct of the event and in accordance with applicable foreign disclosure policy.

b. A Delegation of Disclosure Authority Letter (DDL), a Technology Control Plan (TCP), or other appropriate written guidance, to include email, shall be provided for exercises, training, or experimentation which should include restrictions regarding any equipment that will be used by foreign personnel, or training that will be conducted during the events.

c. Requests for foreign disclosure reviews shall be uploaded to the FDMS of the first FDO in the chain of command. If a command does not have an FDO in the chain of command, requests should be sent to an FDO at Headquarters, USMC (HQMC), Deputy Commandant for Plans, Policies and Operations (DC PP&O), Strategy and Plans Division (PL) or the Deputy Commandant for Information (DC I), Director Intelligence (DIRINT) FDO, as appropriate. Requestors should provide as much detail as possible to expedite the review process. Normally, a decision will be returned in less than 30 days, depending on the complexity of the issue.

Example of Request for Disclosure Authorization

This can be sent via email to the FDO if the Foreign Disclosure Management System (FDMS) is not available.

At a minimum the information below is required: Make sure to attach the document to be reviewed or list talking points that will be discussed/shared.

If the information is marked "Distribution Statement A, unlimited release" or otherwise known to be "public domain" information, as certified as such by a Public Affairs Officer, *the information does not require a foreign disclosure review.*

1. Title. Provide the title or name of the brief (or talking points if no formal brief will be presented), document, or material, that will be discussed/shared.

2. Classification. Identify the highest level of classification required to be disclosed.

3. Disclosure Methods. Will disclosure be oral/visual only or is physical or electronic release of documents/material requested? If release is requested, please justify below and describe method for making the government-to-government transfer.

4. Categories of Information. Specify the NDP-1 categories to be disclosed. (See enclosure (5) of MCO 5510.20C; An FDO can help determine the categories if unsure.)

5. Justification. Why is it important to share this information with a foreign government?

6. Specific government, international organization, coalition, etc. for which disclosure/release is requested?

7. Benefit to the United States. Why is it in the best interest of the United States to disclose/release this information? (May be covered in the justification above.)

8. Suspense Date

9. Additional Comments

10. Point of contact. Phone/email

NDP-1 Categories of Classified Military Information

1. Category 1 – Organization, Training, and Employment of Military Forces. Military information of a general nature necessary to the organization of military, paramilitary, or irregular forces to include those tactics, techniques, and tactical doctrine (including 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.

2. Category 2 – Military Material and 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 in this category. Items on the U.S. Munitions List that 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 including 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.

3. Category 3 – Applied Research and Development Information and Material. Classified military information resulting from the extension of fundamental theories, designs, and data from purely theoretical or experimental investigation into possible military applications, including 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.

4. 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 upgrade substantially military materiel and munitions. The following information is furnished to clarify the definition of Production Information:

a. 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, explosive, 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 which has completed Acquisition Milestone II (Development Approval) or documentation used for production thereof are 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 contain or allow access to or insight in classified algorithms or design rationale are 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, and displays will be handled through normal technology transfer channels and do not require NDPC review. Such information will normally be considered for release to foreign customers that 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.

b. 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 that discloses design methodology, engineering analysis, detailed process information, or manufacturing know-how associated with the end item or 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.

c. 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.

5. Category 5 – Combined Military Operations, Planning, and Readiness. The 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. This category 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 or North American Defense Information.

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

7. Category 7 – North American Defense. North American Defense Information is that concerning 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). North American Defense Information includes but is not limited to:

a. Plans and related documents prepared by the U.S. defense agencies concerning the defense of the United States.

b. Plans and related documents prepared in combination with the Government of Canada, wither bi-nationally (i.e., NORAD) or bilaterally (i.e., between USNORTHCOM and Canada 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 combat readiness of any unit or facility, or the effectiveness of North American Defense systems.

8. Category 8 – Military Intelligence. Military intelligence comprises information of a military character pertaining to foreign nations and areas as delimited by the criteria for the disclosure of intelligence in Section II of NDP-1 (NOTAL).

NDP-1 Disclosure Criteria, Conditions, and Limitations

1. Disclosure Criteria. In accordance with reference (a), disclosure of CMI in Categories 1 through 7 may be made only when all of the following criteria are satisfied (Note: See NDP-1 for additional criteria for Category 8, Military Intelligence information). The examples set forth below are provided for information only and are not intended to reflect sub-criteria that must be met prior to considering that the basic criteria have been met.

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

(1) The recipient cooperated with the United States in pursuance of military and political objectives that are compatible with those of the United States.

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

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

b. Disclosure is consistent with U.S. military and security objectives. For example:

(1) Disclosures of advanced technology, if compromised, will not constitute an unreasonable risk to the United States position in military technology and operational capabilities, regardless of the intended recipient.

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

c. The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the United States. Note: The intent of a foreign government to protect U.S. classified military information is established in part by the negotiation of a General Security of Military Information Agreement (GSOMIA) or other similar security arrangement. Guidance in determining a foreign government's capability to protect U.S. classified military information may be determined by a security assessment, such as an embassy security assessment, CI risk assessment, and/or a National Disclosure Policy Committee (NDPC) Security Survey Report. If no Security Assessment exists, disclosure approval will be considered on a case-by-case basis, with the understanding that a higher standard of justification and rationale for the disclosure of the classified military information will be required for a specific foreign government or international organization when there is no GSOMIA or Security Assessment.

d. Disclosure will result in a clearly defined advantage to the United States. For example:

(1) The United States obtains information from the recipient nation on a quid pro quo basis.

(2) The exchange of military information or participation in a cooperative project will be advantageous to the United States from a technical or other military viewpoint.

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

e. The disclosure is limited to information necessary to the purpose for which disclosure is made. For example, if the purpose of the disclosure is the sale of military equipment, information on operation, maintenance, and training would be released. Research and development data, or production know-how must be withheld.

2. Disclosure Conditions. After a decision is made to disclose CMI to a foreign government or international organization, based on the criteria listed in paragraphs 1c through 1e of this enclosure, above, or an exception to policy, release of the CMI will be contingent upon assurances by the recipient that the listed minimal conditions in the subsections 2a through 2h, below, will be met. The conditions normally are satisfied by the provisions of existing GSOMIAs. When a GSOMIA does not exist, the conditions may be included in a program-specific agreement, government contract, or similar arrangement.

a. The information or acknowledgement of its possession will not be revealed to a third party except with the prior written permission of the originating U.S. department or agency.

b. The information will be afforded substantially the same degree of security protection afforded to it by the United States.

c. The information will be used only for designated military purposes, or other specified purposes, including production for military use when so authorized.

d. The recipient will report promptly and fully to U.S. authorities any known or suspected compromise of U.S. classified military information released to it.

e. All individuals who, and facilities that, will have access to the CMI and material will have security clearances granted by their government at a level greater than or equal to that of the classified information involved and an official need-to-know.

f. The information will be transferred through government-to-government channels.

g. Security experts of each government will be permitted to visit the other government, when mutually convenient, to review and discuss each other’s policies and practices for protecting classified information.

h. The recipient of the information agrees to abide by or meet United States specified special terms and conditions for the release of U.S. information or material.

3. General Disclosure Limitations. Nothing in this Order shall be construed so as to allow the disclosure of the following types of information:

a. Prohibited by Law or Agreement. Classified information, the disclosure of which is prohibited by Federal law or by an international agreement to which the United States is a party.

b. Naval Nuclear Information. Any naval nuclear propulsion information, classified or unclassified, except under an agreement negotiated pursuant to the Atomic Energy Act of 1954.

c. Proprietary Information. Classified or unclassified proprietary information, the rights to which are owned by private firms or citizens (i.e., patents, copyrights, or trade secrets) without the owner's consent, unless such disclosure is authorized by relevant legislation, and then release will be subject to such legislation.

d. National Intelligence. National Intelligence or interdepartmental intelligence produced within the National Foreign Intelligence Board structure. Such intelligence cannot be disclosed without authorization of the Director of National Intelligence.

e. National Security Telecommunications and Information Systems Security Information. The National Security Telecommunications and Information Systems Security Committee is authorized by its terms of reference to make disclosures of classified military telecommunications and information systems security equipment and information without reference to the NDPC.

f. Counterintelligence. Operational information related to counterintelligence activities and disclosures related thereto.

g. Atomic Information. Such disclosures are made in accordance with the Atomic Energy Act of 1954.

h. Strategic Planning and Guidance. Only the Secretary of Defense or the Deputy Secretary of Defense may authorize the disclosure of plans, concepts, or other information about strategic war plans. Requests for such disclosure shall be submitted through the Chairman of the Joint Chiefs of Staff.

i. Specifically Prohibited Disclosures. The following types of classified information are specifically prohibited from disclosure:

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

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

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

(4) Information originated by or for another department or agency, unless that department or agency consents to the disclosure.

(5) Intelligence information described in section I, subparagraph 5.c (2) and section II, subparagraph 5.b (7) of NDP-1 (reference (b)).

USMC International Visits Program Guidance and Procedures

1. General. This enclosure provides specific guidance to disclosure authorities and other USMC personnel who work with foreign visitors for establishing feasibility of support and making disclosure decisions regarding official visits to USMC facilities by foreign nationals. Chapters 11 and 12 of reference (t) provide in-depth DON guidance regarding international visits and should be used to obtain additional guidance, as needed. Reference (d) establishes the International Visits Program (IVP) and provides policy guidance for the control over visits of foreign nationals and foreign representatives of international organizations to all Department of Defense activities and cleared contractor facilities.

a. Official Foreign Visit. An official foreign visit is an occasion when a foreign national is sponsored by his or her government, or by an international organization, to perform official business with the U.S. Government or a cleared contractor facility. Per reference (d), while offering great potential, official visits and assignments of representatives of foreign governments or international organizations also present a risk of unauthorized disclosure or compromise of DoD classified military information (CMI) or controlled unclassified information (CUI), including export controlled technical data and technology, unless prescribed access controls are appropriately applied. The decision to grant access to CMI or CUI during official visits shall be consistent with the security and foreign policy interests of the United States.

b. Unofficial Foreign Visit. Per reference (d), an unofficial foreign visit is an occasion when a foreign national is not sponsored by his or her government or an international organization.

(1) Examples of unofficial visits include: foreign nationals representing private business interests, foreign nationals employed by DoD contractors, and foreign nationals participating in events open to the general public.

(2) Courtesy calls are also considered unofficial visits even if the visitor is an official representative of a foreign government. Courtesy calls shall be limited to general protocol interactions, but shall not involve the disclosure of CMI or CUI. If the courtesy visit has the potential to involve CMI or CUI, then the visit is no longer a courtesy call and shall be treated as an official visit.

2. Policy. Foreign Visit Requests (FVR), also called Requests for Visit Authorization (RVA), are normally required for official representatives of foreign governments or international organizations to visit USMC activities and cleared contractor facilities in the United States, or any location in the United States or abroad in order to discuss official business. Official foreign visitor access must be properly controlled to avoid inadvertent or unauthorized disclosure and to prevent unnecessary disruption to ongoing operations at USMC commands where the visits take place. The final decision to host or schedule a specific visit is at the discretion of the host command or facility. All personnel who work with or have close contact with foreign visitors should familiarize themselves with this Order, references (c) and (d), and Chapters 11 and 12 of reference (t), which provide further guidance for conducting foreign visits.

3. The Foreign Visits System

a. The DoD Foreign Visits System (FVS), operated and maintained by Defense Technology Security Administration (DTSA), provides staffing and database support for the processing and recording of visit requests by foreign nationals to DoD activities or authorized contractor facilities. The FVS consists of three different parts:

(1) FVS-Embassy is an unclassified system that allows foreign embassies to submit a FVR online to the appropriate military department, where it is then drawn into a classified system used by DoD (FVS-DoD).

(2) FVS-DoD is the classified system used by USMC to staff and support the decision-making process surrounding a foreign visit. After a decision has been reached on a specific visit request, the FVS is able to transmit a visit confirmation message to the requesting embassy via unclassified means. The FVS also generates a record of the disclosure decision.

(3) FVS–Confirmation Module (FVS-CM) is a mandatory, Non-secure Internet Protocol Routing (NIPR) network-based program that allows commands to check-in foreign visitors upon arrival and check them out when they depart. FVS-CM is the only system that provides actual data on foreign visits by tracking them against approved FVRs in FVS-DoD. It documents that the visit took place, the names of foreign individuals who actually visited, and the substance of discussions or disclosures made during the visit, in accordance with reference (y), as provided by the Contact Officer. It is also a means to document unclassified, unofficial visits or unannounced visits to commands when no FVR can be found in FVS and the command chooses not to turn the visitor away for political or other reasons. Commands can obtain guidance to establish accounts in FVS and FVS-CM by calling the Security Policy Automation Network (SPAN) help desk at commercial (571) 372-7623, DSN 372-7623, or by sending an email to dtsaspansupport@dtsa.smil.mil.

b. All USMC commands or activities which receive at least three foreign visits per year shall use the FVS-DoD and FVS-CM.

(1) All FVRs shall be staffed via the FVS. Email notifications of pending FVRs may be set up with the SPAN help desk, however, all official actions shall take place in the FVS. Email responses will not be accepted, except in emergency or other unusual situations.

(2) Commands shall have only one account in FVS to eliminate confusion when staffing visits and to ensure the appropriate persons within the command have visibility and control of visits. If a command currently has more than one account, notify DC I (DIRINT) and DC, PP&O (PL) of the appropriate account to use for staffing visits. Multiple individuals may hold logins for the one command account.

c. Commands that receive less than three foreign visits per year should request that senior USMC commands record the visit information in FVS and FVS-CM.

d. The FVS recognizes the following types of official visits by foreign nationals or their representatives, under the sponsorship of their government or an international organization, to a DoD component or DoD contractor facility:

(1) One-time Visits. The one-time visit request should be submitted to the HQMC Office of Primary Responsibility (OPR), DC I (DIRINT), no less than fifteen calendar days prior the visit start date, but are not required more than thirty calendar days prior to the visit start date. A one-time visit will not exceed thirty days. Emergency visits are those one-time, short notice visits that are submitted by the foreign government or international organization, normally less than fifteen calendar days prior to the visit, and are identified as such. An emergency visit request will be limited to situations in which failure to conduct the visit will jeopardize an official government project, program, or contract. The request will not be accepted less than one full working day prior to the visit. Since the concurrence of the host facility is always required, obtaining their tentative approval in advance will expedite the processing of the emergency visit request. Emergency visit requests should not be submitted to circumvent routine visit procedures.

(2) Recurring Visits. A recurring visit will not exceed one year in duration, and acceptance by the host facility will be program-dependent or as specified by local facility policy. The recurring visit request should be submitted as soon as possible, but is not required more than thirty calendar days prior to the visit start date. DC I (DIRINT) is the OPR for recurring visits. Apart from emergency visits, the recurring foreign office or visitor(s) shall give the host activity at least a 72 hour notice of the actual date and time of the intended visit following approval of the recurring FVR. All activities have the right to refuse any visit if the visitor arrives without such notice.

(3) Extended Visits. An extended visit is approved by the HQMC Office of Primary Responsibility (OPR), DC PP&O (PL). Extended visits are normally submitted in support of an on-going international agreement, contract, or program when the visitor is required to be on continuous assignment with a USMC activity, usually for 2 to 3 years. This type of FVR is used for programs such as Foreign Liaison Officer (FLO), Personnel Exchange Program (PEP), or Cooperative Program Personnel (CPP) assignments. Hosting organizations shall resubmit extended visit personnel for screening and vetting each year, on the anniversary of their initial screening, for the duration of their assignments.

e. Visit Amendments. The requesting embassy may amend official visit requests. Amendments are limited to the date(s) of the visit and/or the names of the visitors. If any other element of the visit request requires an amendment, a new visit request must be submitted. Emergency visits may not be amended. The Office of Primary Responsibility, explained below, shall make every effort to submit new names to MCIA for screening and vetting upon receipt of a visit amendment.

f. Office of Primary Responsibility (OPR). An OPR, as it relates to the foreign visit approval process, will make decisions based upon review of applicable policies and the staffing recommendations received, and enter any applicable disclosure restrictions and guidance into the FVS as recommended by the host commands. As outlined above, DC PP&O (PL) normally acts as OPR for extended visits and DC I (DIRINT) normally acts as the OPR for one-time and recurring visits.

g. The FVS has a downloadable user guide to assist in navigating the program; the SPAN help desk and DC I (DIRINT) can also assist with specific questions about the system.

4. Exemptions to the FVS. The following types of visits are exempt from the FVR process:

a. Unofficial Visitors. Visits by foreign nationals, whether government officials or industry civilians, who are not representatives of their government in an official capacity are exempt from the visit request process. These visits shall be governed by local security practices in accordance with standard physical and operational security requirements.

b. Unclassified Information at Contractor Facilities. Visits conducted at DON contractor facilities that involve access to only unclassified information. This exemption is subject to the following three limitations:

(1) In some cases, a government contract will require a contractor to administer all foreign visits to its facilities via the FVS. When a contractor has an obligation of this nature, FVRs must be submitted by the parent embassy of the proposed foreign visitor.

(2) The subject matter of the proposed visit must be unrelated to DON programs.

(3) The contractor holds a valid export license, or the information to be disclosed does not require an export license.

c. Visits by Foreign National Contractors. Reference (z) regulates visits by foreign national employees of U.S. defense contractors. Access to export-controlled technical data by foreign national employees of U.S. contractors is authorized in accordance with an export license or by another written U.S. Government authorization that the employing contractor obtains. When these employees visit another contractor facility or DON component, the employing facility should provide a copy of the export license or other written authorization to the security office or FDO of the host facility.

d. Invitational Travel Orders (ITOs). Visits by foreign nationals to participate in security assistance training using ITOs provided by their in-country U.S. Security Cooperation Office are exempt from the FVS. Within the USMC, the FVS shall not be used to seek disclosure authorization for disclosing training course information to foreign governments, international organizations, or their representatives. Training-related disclosures are covered in Chapter 10 of reference (t).

e. Unclassified Orientation Tours. Visits by foreign nationals traveling on ITOs for Orientation Tours arranged under the Security Assistance Training Program (SATP) when CMI will not be disclosed are exempt from the FVS. If disclosure of CMI is required as part of the orientation tour an FVS request must be submitted by the foreign visitor’s embassy in Washington, D.C. to certify the visitor’s security clearance.

f. United States/Canada Joint Certification Program (JCP). Unclassified visits by Canadian government officials and certified Canadian contractors through the United States/Canada JCP are exempt per reference (aa).

g. Joint Contact Team Program. Visits sponsored and administered by the U.S. European Command under its Joint Contact Team Program are exempt if the visitors are traveling on ITOs and no CMI will be disclosed.

h. Professional Development Orientation and Familiarization Tour Programs. Unclassified visits that fall under the auspices of Professional Development Orientation and Familiarization Tour Programs conducted by Unified Commands, fleet commanders, or USMC component commanders, and that are funded using Traditional Combatant Commander (COCOM) Activities resources, are exempt. If disclosure of CMI or CUI is anticipated, then a visit authorization is required.

i. Unclassified DON Employment of Foreign Nationals. The long-term unclassified employment of foreign nationals is exempt per reference (t).

j. CMC and Chief of Naval Operations (CNO) Counterpart Visits are exempt from embassy submission of FVRs. Arrangements for visits by the heads of foreign Navies and foreign Marine Corps conducted through this program are the overall responsibility of CMC and managed by DC PP&O (PL) and DC I (DIRINT) in the USMC. Upon notification by DC PP&O (PL), DC I (DIRINT) will input an FVR into the FVS and provide disclosure guidance for the counterpart visit. DC PP&O (PL) will then disseminate the disclosure guidance, as required, to those activities hosting the CMC counterparts and entourage.

k. Public Areas or Locations. Visits to areas or locations accessible to the public are exempt when they only involve information officially approved for public release. Official meetings in commercial facilities (e.g., hotel conference facilities) that entail the disclosure of CMI or CUI requires the submission of a FVR and the same level of disclosure review as meetings held at USMC or cleared contractor facilities. Meeting hosts should coordinate with information and physical security professionals when planning the meeting.

l. Virtual Visits. Telephone, Video TeleConference (VTC), secure VTC, Tandberg, and other virtual communication or meetings are exempt. Any CMI or CUI to be disclosed requires the same level of disclosure review as meetings held at DON or cleared contractor facilities.

5. FVS Disclosure Review Process. Official foreign visitors may be permitted access to CMI or CUI that is authorized for disclosure to their parent governments and necessary to the stated purpose of their visit. Only an FDO or other official delegated authority by an appointment letter from a commander or director holding a Delegation of Disclosure Authority Letter (DDL) may approve access to CMI and CUI by visiting foreign nationals.

a. Process Initiation. The FVS process begins when a foreign embassy, located in Washington DC, or the designated office of an international organization submits a FVR to visit a USMC component. FVRs are required to be submitted no less than 21 working days prior to the first day of the proposed visit.

(1) Embassies with terminals connected to DoD's SPAN FVS-Embassy must submit their visit requests electronically. The FVS automatically forwards to DC I (DIRINT) visit requests to USMC commands, activities, and contractor facilities under contract to the USMC.

(2) Embassies or international organizations without FVS connectivity shall submit visit requests via facsimile to DC I (DIRINT) in accordance with the procedures set forth in reference (ab). DC I (DIRINT) will then enter the requests into the FVS.

b. Staffing and Review. The OPR shall staff the FVR using the disclosure procedures outlined in reference (t) and this Order. The knowledgeable U.S. point of contact designated on the FVR should be able to evaluate the subject/justification in the FVR and assist the OPR and the FDO in developing disclosure guidance and feasibility of support. In those cases where the identified knowledgeable U.S. point of contact is not the appropriate reviewing point of contact for the subject matter designated in the FVR, the OPR or the FDO, as appropriate, shall either attempt to locate the appropriate knowledgeable U.S. person or return the visit to the embassy for correction. FVRs that have been incorrectly assigned and fall under the cognizance of another OPR shall be transferred online directly to the proper OPR.

c. Foreign Disclosure. It is imperative that an initial foreign disclosure assessment is conducted before the visit is recommended for approval in the FVS so that the anticipated classification level for the visit and information to be disclosed is properly documented in the approved FVR. The command FDO and/or FDR shall be included in the planning process of the visit, in coordination with the knowledgeable U.S. point of contact, to ensure that all materials and information to be disclosed have been properly identified and reviewed/approved before the visit takes place.

d. OPR Decision. The OPR will make a decision on each FVR based upon a review of applicable policies and the recommendations received from staffing, screening, and vetting, when appropriate. Although the final decision for hosting an official visit during the requested timeframe is at the discretion of the host command or facility, their decision does not provide authority for them to actually host or deny the visit or to disclose information without the final visit adjudication in the FVS. Only an OPR may adjudicate visit requests using one of the following decision inputs for each FVR:

(1) Approval. The OPR shall enter the approval decision, the approved level of classified disclosure provided by the FDO, and general disclosure guidance. Once the OPR closes the request in the FVS, the system automatically notifies the embassy or international organization of the approval but the foreign embassy does not receive any notice of the disclosure/classification level for the visit or any of the disclosure limits stipulated by the OPR/FDO.

(2) Denial. The OPR must judiciously apply this option because denial may result in political, cultural, or military repercussions. An OPR may only deny a FVR when policy precludes the visit to take place.

(3) Return Without Action. If a visit request is incomplete or the visit cannot be approved for any reason other than that which is disclosure policy related, the OPR shall return the request to the embassy with an accompanying explanation. By returning the request with comments, the visit can be edited and resubmitted by the sending embassy or organization without having to initiate an entirely new request. For example, if the return without action is due to a scheduling conflict, the OPR might wish to recommend alternate dates for the visit.

(4) Return Without Sponsorship ("non-sponsored"). If the visit request is for a visit to a contractor facility and the OPR cannot identify any specific USMC program or contract that supports the visit, the OPR may return the request without sponsorship. The lack of sponsorship does not prevent the visit, but merely denotes that the visit is not related to a USMC program or contract.

(5) Cancellation. Either the OPR or the requesting embassy may cancel a visit request. This is an administrative action that removes visit requests because of a change in schedule or other circumstances. It also allows either party to remove duplicate visit requests.

e. Disclosure Restrictions or Limitations. The disclosure authorization will set a classification level that cannot be exceeded during a visit. If the objectives of the visit can be accomplished by the disclosure of information at a lower classification level than that authorized in the visit approval notification, it is the responsibility of the host(s) to limit the disclosure accordingly.

f. Disclosure Authority. A visit authorization does not include authority to physically or electronically provide documents to a visitor, unless that authority has been explicitly granted within the disclosure authorization by an FDO.

g. Visit Amendments. The OPR should review the FVS "Amendment" folder daily to see if any cases have been amended. When a visit is amended, the FVS is updated to reflect the amendment, but the FVS does not automatically notify the OPR that an amendment has been made to a visit. The requesting embassy may amend the visit request with respect to the date(s) of the visit and/or the names of the visitors only. If any other element of the visit request requires an amendment, a new visit request must be submitted.

6. General Host Command Guidance for Foreign Visits

a. Foreign Visits Coordinator. Each command or facility that receives three or more foreign visits per year shall appoint a foreign visits coordinator who is responsible for logging into the FVS on a daily basis, staffing FVRs to the host facilities, and providing a recommendation to the OPR for each visit under their cognizance. The foreign visits coordinator can be the FDO, the security manager, or other person designated by the commander to run the local IVP, as determined by local policy. At a minimum, local policy should include:

(1) Physical Security and Facility Access. Security Managers must be involved in foreign visit planning to provide guidance on visitor access to the host activity. Local base or facility badging regulations shall apply to all one-time and recurring official foreign visitors.

(2) Appointment and training of Contact Officers. FDOs shall ensure that the appropriate number of Contact Officers, also known as "escorts" for one-time or recurring foreign visits, are assigned and trained. FDOs should train a deep bench of command personnel to act as Contact Officers so that emergency or other short-turn visits can be expeditiously handled with minimum disruption to the command mission. Further information regarding duties and responsibilities of Contact Officers can be found below in this enclosure and in enclosure (8). Qualifications for contact officers should include:

(a) Must be equal or higher in rank than the foreign visitor assigned to them (except in the case of general/flag officers who may be escorted by a colonel, a field grade officer, or a civilian equivalent). Local command foreign disclosure/foreign visit policy may provide additional exceptions to this requirement when necessary due to local circumstances.

(b) Must be trained by the FDO on local procedures and must complete the MarineNet Contact Officer Course.

(c) Be responsible and represent the host command and the USMC well.

(d) Be culturally aware about the customs of the visiting country so as not to unknowingly offend the foreign visitor.

(3) Terrorist and Criminal Screening. To ensure compliance with reference (t), all USMC entities are responsible for ensuring that all foreign personnel under their cognizance are screened for terrorist and criminal associations prior to arrival, and that their arrival and departure dates are documented in an automated system that feeds specific foreign visitor data into the DoD Cornerstone system. The requirement for documentation is met when an FVR is submitted into the FVS and subsequently approved. Reference (t) further requires that all DoD components shall cooperate with DoD intelligence, counterintelligence, law enforcement, and security elements to ensure the stay of DoD-hosted foreign personnel is as secure and safe as possible for all parties. For all non-FMF (supporting establishment) entities HQMC will assign FVRs to MCIA to provide support to entities without organic intelligence or counterintelligence elements through the Counterintelligence Analysis Cell (CIAC), and the Identity Analysis Cell (I2AC) in screening and vetting of foreign visitors. The CIAC and I2AC, as part of MCIA, are responsible for providing counterintelligence and identity-based analytic support to those same service-retained entities to include screening and vetting of foreign visitors to determine whether they present a terrorism threat. All USMC entities can request support for screening or vetting from MCIA through the DON Identification and screening Information System (DONISIS) via: https://isis.identityops.com (NIPR) or https://isis.navy.smil.mil (SIPR). When a single request including more than thirty visitors is expected, prior coordination with MCIA is necessary to ensure enough resources can be brought to bear to respond adequately to such a sizeable request.

(4) CI Screening. All foreign visits conducted under the cognizance of this Order shall be subject to an appropriate counterintelligence name check by an authorized counterintelligence analysis cell at either MCIA or the appropriate Marine Expeditionary Force.

7. Host Command Responsibilities for One-time and Recurring Visits

a. Contact Officers/escorts. Serious consideration should go into determining the exact number of Contact Officers/escorts that will be assigned to properly oversee one time or recurring foreign visitors. Several factors, such as the size of the group of foreign visitors, the sensitivity of the areas of the command that they will enter, and whether they will have access to equipment or systems must be considered to ensure each foreign visitor has proper supervision during the entire visit. The Contact Officer/escort for one-time and recurring visits is responsible for controlling all activities and for escorting the foreign visitor(s) at all

times during the visit, as well as ensuring that the disclosure of CMI and CUI strictly conforms to that approved by the FDO. The Contact Officer must be provided a copy of the one-time or recurring visit authorization prior to the visit, and should verify with the command visit coordinator that the list of visitors is current, including amendments. Contact Officers shall ensure visits are documented in the FVS-CM, including a short summary of what was disclosed during the visit in accordance with reference (y). When hosting foreign delegations, commands must make efforts to ensure the success of the visit regardless of size, duration, or seniority.

b. FDOs. Command FDOs must be involved in planning for all foreign visits and must review, approve, and properly mark all CUI or CMI that will be disclosed to one-time and recurring foreign visitors. The FDO should ensure that the appropriate number of Contact Officers/escorts for one-time and recurring visits are appointed and trained. Appointment for one-time and recurring visits is not required to be in writing.

c. Visit Procedures. The host command shall establish local visits coordination procedures which outline the internal staffing process for foreign visits.

d. FVS Accounts. The host command must establish a single account in FVS-DoD and in FVS-CM, with individual logins for the foreign visits coordinator and any other personnel in the command that need access to that account.

e. Security Measures. Security measures should be established to include participation in oversight briefs and/or CI briefs for Contact Officers and all personnel that will come in contact with foreign personnel.

8. Host Command Responsibilities for Extended Visits.

a. Contact Officers. A primary and at least one alternate U.S. Contact Officer must be appointed in writing for all extended foreign visitors, to include Personnel Exchange Program (PEP), Foreign Liaison Officers (FLO), Engineer and Scientist Exchange Program (ESEP), and Cooperative Program Personnel (CPP).

(1) The following documents must be completed and maintained by Contact Officers, with copies forwarded to the command FDO or the first FDO in the chain of command and to DC PP&O (PL).

(a) Contact Officer Assignment Letter

(b) Contact Officer Acceptance Letter

(c) MarineNet “Contact Officer Course” certificate of completion

(d) Appropriate Understanding of Conditions and Responsibilities Letter signed by the extended foreign visitor. Note: Examples of the above listed letters, except the Contact Officer Course certificate, can be found in enclosure (9). PEPs additionally must complete the LIMDIS Non-Disclosure Agreement. Templates for all documents can be found on the DC PP&O PL foreign disclosure SharePoint site: https://eis.usmc.mil/sites/hqmcppo/PL/PLA/PLFD

(2) Extended Visit Primary/Alternate Contact Officer Responsibilities. Contact officer responsibilities for extended foreign visits include:

(a) Control access to CUI and CMI in accordance with the Delegation of Disclosure Authority Letter (DDL) for that billet, references (a) through (c) and (t), local command policy, and in coordination with FDOs, as needed.

(b) Become the subject matter expert regarding the DDL and the FVR and provide guidance to all personnel who will have contact with the assigned foreign personnel.

(c) Coordinate all foreign disclosure that is not clearly outlined in the DDL with the command FDO or FDR or, if one is not assigned, the first FDO or FDR in the chain of command.

(d) Coordinate FLO actions and requests for information with appropriate stakeholders and the FDO, as required.

(e) Coordinate all visits by FLOs to commands outside of their permanent duty stations with the host commands, ensure approved one-time or recurring FVRs are in place, and that disclosure guidance has been passed to Contact Officers/escorts at the host commands.

(f) Provide proper turnover with replacement Contact Officers/alternate Contact Officers and notify the chain of command, including the FDO, about possible gaps in coverage.

(g) Maintain copies of appropriate international agreements regarding the PEP/FLO assignments; contact DC PP&O (PL) for the latest copies of agreements or find them on the DC PP&O (PL) Foreign Disclosure SharePoint site.

(h) Provide the DDL to commands that host one-time or recurring visits by PEPs for visits that are in the line of duty for the PEP billet. Note: One-time or recurring FVRs are not required for PEPs who visit other DON commands, but may be required for visits to other services or activities.

(i) Complete Contact Officer training as prescribed by the command FDO or DC PP&O (PL). MarineNet Foreign disclosure courses are available by searching "Foreign Disclosure."

(j) Contact the nearest Marine CI Element to schedule a defensive CI briefing prior to the arrival of the foreign visitor(s).

9. Foreign Visits Requiring Special Arrangements. The following types of visits necessitate additional considerations and/or special processing:

a. Intelligence-Related Visits. Requests for visits to HQMC DC I (DIRINT), will be transferred to the DC I (DIRINT) OPR for action. Any visit requests outside of DC I (DIRINT) that involve the potential disclosure of intelligence information that would exceed the authority of the cognizant OPR will require coordination with DC I (DIRINT) for final action.

b. Embarkation of Foreign Personnel on USN/USMC aircraft or U.S. ships. See Chapter 6 of reference (t) for specific procedures.

c. Visits to Contractor Facilities. The disclosure of classified information or certain controlled technical data to foreign nationals qualifies as an export under U.S. law and regulations per reference (k). A State or Commerce Department export license is required of all U.S. contractors for the export of classified and export-controlled unclassified information disclosed during foreign visits, unless a DoD component sponsors the visit or an export license exemption applies.

10. Visits to USMC Commands and Facilities Outside of the United States. Control of visits to USMC commands and facilities outside the United States will be treated the same as visits within the United States and will require the use of the FVS-DoD and FVS-CM, as applicable.

Additional Guidance Regarding Extended Foreign Visits

1. Extended Visit. An extended visit is processed with a long-term FVR from the visitor's parent government to a single USMC facility. Extended visits are normally established in support of an ongoing international agreement, contract, or program when the visitor is required to be on continuous assignment with a USMC activity or a DoD contractor facility. This type of FVR is used for such programs as Personnel Exchange Program (PEP) personnel, Foreign Liaison Officers (FLO), or Cooperative Program Personnel (CPP).

2. FVR Submission and Processing Requirement. The visit request submission and processing requirements for extended visits are the same as those established for one-time and recurring visits, with the main difference being that extended visits should be submitted a minimum of 45-days in advance of the commencement date of the assignment. An FVR is required for all extended visitors regardless of location (e.g., overseas and United States facilities).

3. Delegation of Disclosure Authority Letter (DDL). DDLs for PEPs, FLOs, and CPPs are written by DC PP&O (PL) and/or DC I (DIRINT), as required, based on an approved billet descriptions. FDOs with cognizance over an activity with an extended visitor who is not identified as a PEP, FLO, or CPP shall create a DDL for each extended visitor's billet (not the individual filling the billet) based on the billet description, the level and type of information required for their duties, and the ability under National Disclosure Policy (NDP-1) to share at that level with the visitor's parent government. Per reference (a), exceptions to NDP-1 shall not be granted to accommodate the assignment of FLOs, PEPs, CPPs, or foreign personnel arrangements. DDLs provide detailed foreign disclosure guidance to commands that host extended visits. The contents of the disclosure authorization shall not be disclosed to the foreign visitor. This prohibition does not preclude the host from informing the visitor of the upper limit of the access being authorized during the assignment in general terms, however, under no circumstances will specific disclosure limitations be revealed to the extended visitor.

4. Types of Extended Foreign Visitors. Extended foreign visitors include:

a. Foreign Liaison Officer (FLO). A FLO is an officer or enlisted representative of a foreign military organization assigned by his or her government to a USN/USMC activity with DON approval. A FLO works only for his or her parent foreign government and represents its interests to the DON and may never perform U.S. Government duties or responsibilities. FLOs may be categorized into three types:

(1) Security Assistance FLOs may be assigned to DON activities to oversee Foreign Military Sales (FMS) implementation. These assignments must be covered through an FMS Letter of Offer and Acceptance (LOA) that establishes a FLO requirement, an international Memorandum of Understanding (MOU), or a Memorandum of Agreement (MOA).

(2) Operational FLOs may be assigned as an interface between their command elements and a U.S. command in support of operational matters such as combined operations and planning. These assignments must be implemented via an MOU/MOA that establishes the FLO requirement. The Commandant of the Marine Corps (CMC) shall be responsible for the establishment of Operational FLO MOUs/MOAs and may further delegate this function as he deems appropriate.

(3) National Representative FLOs may be assigned to their national embassy or diplomatic mission as military attachés to conduct liaison activities with the USMC. These FLOs do not require extended visit authorizations, nor DDLs. They do, however, require an approved visit authorization per reference (t) when making one-time or recurring visits to USMC facilities and discussing substantive or technical matters, or classified or controlled unclassified information.

b. Personnel Exchange Program (PEP). The PEP encompasses all exchange programs that include the assignment of officer, enlisted, or civilian foreign nationals to positions within DoD components under an approved billet or position description, and the terms of a bilateral or non-reciprocal personnel exchange agreement. PEPs may be categorized into four types:

(1) Military PEP. This program includes all assignments of foreign military personnel to authorized USN/USMC billets, normally on a reciprocal basis.

(2) Engineer and Scientist Exchange Program (ESEP). This program includes all assignments of civilian and military engineers and scientists to DON Research, Development, Test, and Evaluation (RDT&E) facilities.

(3) Administrative PEP. This program includes all assignments of civilian and military specialist personnel to administrative, logistics, finance, health, legal, and planning billets within DON.

(4) Defense Intelligence PEP. This program includes all assignments of military intelligence personnel within the USMC intelligence community. The Director, Defense Intelligence Agency (DIA) has been designated as the Executive Agent for this program. All assignments under this program to USMC activities are coordinated through USMC intelligence organizations as appropriate. DDLs will be issued by DC I (DIRINT) in accordance with DIA-provided direction and procedures.

c. Cooperative Program Personnel (CPP). CPPs are foreign nationals (military or civilian employees of the counterpart foreign government defense establishments) assigned to bilateral or multilateral program or project offices that are hosted by a DON activity. They may be assigned as a part of international project management staff or as a national representative per the terms of the international agreement. To qualify as a CPP, foreign government representatives:

(1) Must be assigned to an international program or project office hosted by a DON component per the terms of an international agreement, and in accordance with reference (r) when applicable.

(2) Must report to and take direction from a DoD-appointed U.S. Program or Project Manager (or equivalent).

(3) Must not be a foreign government representative described as a liaison officer or observer

d. Special Exchanges. In rare circumstances there may be an extended foreign visitor who is not a participant in one of the established programs discussed above. This will occur only after careful review and determination by DC PP&O that it is in the best interests of the United States to do so.

For example, an extended visit request may be approved to support a subject matter expert exchange for 3-6 months. The local FDO must provide foreign disclosure guidance for these special exchanges. DC PP&O (PL) or DC I (DIRINT) will not normally write DDLs for these special exchanges.

4. Procedures Applicable to All Extended Visitors. The following procedures apply to all USMC extended visitors.

a. Unescorted Access. Extended visitors shall be granted unescorted access, during normal working hours, to USMC facilities, or areas within USMC facilities where access is controlled, only when security measures are in place to control access to applicable information and operations within the facility beyond what is authorized in their DDL.

b. Escorted Access. Extended visitors may be authorized escorted access to any space for which they are cleared when the host facility's commanding officer has determined that they have an operational, program, or technical requirement, and where access is within the scope of their DDLs. The Commanding Officer is responsible for securing any information within those spaces that is not releasable to the visitor.

c. Identification. If not easily identified by their uniforms, extended visitors must wear a badge or pass that clearly identifies them as foreign nationals. The host command must ensure that the foreign visitors are clearly identified as foreign nationals when dealing with others through oral, written, and electronic communications. If provided email accounts, foreign nationals must be clearly identified as to their country of origin and the billet that they hold. The email address shall comply with established DoD naming conventions. Specific guidance is normally provided in the DDL.

d. Information Systems (IS). Extended visitors shall not have access to IS unless all materials on the IS are sanitized or protected so that the only material available to the visitor is authorized for disclosure by their DDL.

e. Prohibited Access. Extended visitors shall not have uncontrolled access to classified message traffic, library facilities, card catalogues, or databases. They shall not have access to bibliographies with listings of classified publications per reference (t).

f. Access to Cryptographic Materials. Foreign visitors shall only have access to cryptographic spaces, equipment, or material when authorized by the National Security Agency (NSA) in coordination with USMC Systems Command or DC PP&O (PL). Security clearances passed through Special Security Officer (SSO) channels do not constitute a disclosure or access authorization for cryptographic materials.

g. Custody of CMI or CUI. Extended visitors are not to possess classified information unless explicitly authorized by the DDL. They shall not have custody of CMI or CUI except during normal duty hours at their place of assignment, when such access is necessary to perform their assigned duties, and then only when the information is authorized for disclosure.

h. Interaction with Contractors. The disclosure of classified information or certain controlled technical data to extended foreign visitors by U.S. contractors may qualify as an export under reference (k) or (q). A State or Commerce Department export license or exemption may be required of

U.S. contractors for the export of classified and export-controlled unclassified information disclosed to extended foreign visitors.

i. Responsibilities and Prohibitions for FLOs. An MOU, MOA, or LOA formally establishes the legal basis for the FLO position(s) and covers such matters as the responsibilities and obligations of the governments, authorized activities, security requirements, financial arrangements, and claims. The MOU, MOA, or LOA also establishes that the duties of the FLO shall be limited to representational responsibilities for his or her government per the agreement by which the billet is established.

(1) A FLO shall not perform any activities that are the responsibility of an employee or command element of the U.S. command or facility to which they are assigned. They may not be tasked by the command; they may not be assigned a command job code or title (that might imply that they are representing the USMC or the U.S. Government); and they should not be provided command uniform name tags.

(2) A FLO may not represent the USMC in any capacity and may not enter any contracts on behalf of the USMC or the U.S. Government.

(2) FLOs may not take custody of documentary information except as couriers. They may only act as couriers when they are authorized in writing to serve their government as couriers, and then only when the documentary information has been approved for disclosure to their government.

(4) FLO disclosure guidelines are contained in the billet DDL. A FLO may have access to CMI or CUI in accordance with the DDL upon approval of their extended visit request in the FVS.

(5) Extended visit authorizations for a FLO will be limited to the command or activity to which the individual is assigned. All visits by FLOs to commands and activities other than the one to which they are assigned require the approval of an FVR submitted by the FLO's parent government.

j. Responsibilities and Prohibitions for PEPs. Whether military or civilian, foreign personnel assigned to PEP positions shall be integrated into the U.S. workforce at the USMC host command subject to the limitations outlined in the DDL. They shall neither act as representatives of their parent government, nor act as a conduit for the exchange of CMI or CUI.

(1) PEPs shall not exercise responsibilities that are reserved by law or regulation for an officer or employee of the U.S. Government. For example, PEPs shall not perform the responsibilities of a contracting officer, a security officer, or escort for foreign national visitors.

(2) PEPs shall not be assigned to positions that would result in their access to CMI or CUI which has not been authorized for disclosure by their DDL, or that exceeds the levels authorized for disclosure to their government by USMC policy or NDP-1. A PEP's integration into the workforce does not alleviate this disclosure limitation. PEP disclosure guidelines are contained in the billet DDL. PEPs may have access to CMI or CUI upon approval of their extended visit requests in the FVS.

(3) Visits or Temporary Duty (TDY) Assignments

(a) PEP visit authorizations will usually be limited to the command or activity to which the individual is assigned and any subordinate commands. Visits to USMC commands or activities not subordinate to the host command, or to appropriate DoD contractor facilities may, however, be authorized and arranged by the host command when the purpose of the visit falls within the scope of the PEP's billet description in the DDL. The Contact Officer is authorized to communicate directly with the activity to be visited to arrange the visit, subject to the host command's concurrence.

(b) Visits by PEPs to commands and activities for a purpose outside the scope of their billet description should be rare and will normally be denied except under unique circumstances.

k. Responsibilities and Prohibitions for CPPs. An International Agreement (IA) such as an MOU or MOA formally establishes the legal basis for the CPP position(s) and covers such matters as the responsibilities and obligations of the governments, authorized activities, security requirements, financial arrangements, and claims.

(1) A CPP is assigned to a specific cooperative program or project and shall not perform any activities of the host or parent U.S. command or facility outside of the scope of the project. They should not be assigned a host or parent command job code or title that might imply that they are representing the USMC or the U.S. Government.

(2) CPPs shall not act in a dual capacity as an official/employee in the international program office and a liaison officer for their government (e.g., FLO) while assigned to a DON component. See reference (t) for possible rare exceptions to this policy.

(3) CPPs shall not be assigned to positions reserved by law or regulation for an officer or employee of the U.S. Government. For example, they shall not perform as a U.S. contracting officer, a component duty officer, a security officer, or escort for foreign nationals.

(4) CPPs shall not be assigned to positions that could result in their access to CMI or CUI that has not been authorized for release to their government and that is outside of the scope of information disclosed to their assigned cooperative program or project. CPPs serving as couriers between the USMC and a foreign government for requests and transmissions of CMI and CUI shall act in accordance with the terms of the cooperative program or project's Program Security Instruction. CPP disclosure guidelines are typically contained in the program or project DDL. A CPP may have access to CMI or CUI in accordance with the DDL upon approval of their extended visit request in the FVS.

(5) Extended visit authorizations for a CPP will be limited to the command or activity to which the individual is assigned. All visits by CPPs to commands and activities other than the one to which they are assigned require the approval of an FVR submitted by the CPP's parent government. Disclosure guidance for external commands or activities shall be contained in the approved visit authorization.

l. Extended Visitor Training. Per reference (t), PEPs may not receive formal training except as necessary for familiarization, orientation, or

certification regarding unique aspects of the positions to which they are assigned. Initial training required prior to assuming the duties of a PEP assignment may be conducted through an FMS case via Invitational Travel Orders (ITO). Care should be taken to ensure proper transition from the ITO authorities to an approved extended FVR and a DDL. FLOs and CPPs shall not receive training unless the U.S. Government is reimbursed for the costs of such training.

Examples of Contact Officer Documents

SSIC/Ser
Date

From: Commander (HOST COMMAND/UNIT)
To: (APPOINTEE NAME)

Subj: APPOINTMENT AS CONTACT OFFICER

Ref: (a) Insert Serial Number/date of applicable Delegation of Disclosure Auth Letter (DDL)
(b) DoDD 5230.20 of 22 Jun 2005

1. In compliance with the provisions of the references, you are hereby designated as the Contact Officer for (NAME OF PEP/FLO), HOME SERVICE).

2. In the performance of your duties as the Contact Officer for (NAME OF PEP), you shall maintain complete familiarity with the content of the references and comply with the provisions set forth therein.

3. Unless otherwise directed by separate correspondence, your appointment as the Contact Officer for (NAME OF PEP/FLO) will be relinquished upon termination or transfer to another position.

SIGNATURE LINE

FIRST ENDORSEMENT

From: APPOINTEE NAME
TO: (Commander or Chief of Staff w/By Direction Authority)

1. I hereby acknowledge my responsibilities as the Contact Officer for (NAME OF PEP/FLO, HOME SERVICE). I understand I am to maintain complete familiarity with the references.

SIGNATURE LINE

Copy to: (Edit As Needed)
(Command) FDO

ACCEPTANCE OF CONTACT OFFICER DUTIES FOR (NAME OF PEP/FLO), (NATIONALITY)

I accept the designation of U.S. Contact Officer and fully understand the duties and responsibilities associated with this assignment. I also understand that I must ensure that:

1. (NAME OF PEP/FLO) understands the terms of his certification agreement, including responsibilities and limitations.

2. (NAME OF PEP/FLO) is provided access only to that U.S. classified and controlled unclassified information that has been authorized for release to his government and is necessary to fulfill the terms of his assignment.

3. U.S. co-workers and others with whom he has contact are informed of the limitations on access to U.S. information by (NAME OF PEP/FLO) and their responsibilities in dealing with him.

Print Rank/Name_____

Signature_____

Date_____

PERSONNEL EXCHANGE OFFICER'S (MCFPEP) CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES

I understand and acknowledge that I have been accepted for assignment to (HOST COMMAND) in (CITY, STATE) pursuant to an agreement between the (HOME SERVICE) and the United States Department of Defense. In connection with this assignment, I further understand, acknowledge and certify that I shall comply with the following conditions and responsibilities:

1. The purpose of the assignment is to gain knowledge of the organization and management of activities at (HOST COMMAND). There shall be no access to information except as required to perform the duties described in the billet description of the position to which I am assigned, as determined by my designated supervisor.

2. I shall perform only functions that are properly assigned to me as described in the Billet Description for my assignment and shall not act in any other capacity on behalf of my government or my Parent Party of Parent Organization.

3. All information to which I may have access during this assignment shall be treated as information provided to my government in confidence and shall not be further released or disclosed by me to any other person, firm, organization or government without prior written authorization of the U.S. Department of Defense.

4. When dealing with individuals outside of my immediate office of assignment on official matters, I shall inform such individuals that I am a foreign exchange person.

5. I have been briefed on, understand, and shall comply with all applicable security regulations of the U.S. Department of Defense and the Host Organization.

6. I will immediately report to my designated supervisor all attempts to obtain classified, proprietary or controlled unclassified information to which I may have access as a result of this assignment.

Print Rank/Name_____

Signature_____

Date_____

FOREIGN LIAISON OFFICER'S (FLO) CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES

1. LIAISON OFFICER LEGAL STATUS OF CERTIFICATION: As a representative of the [*Name of Parent Party and, as applicable, the Parent Party command or organization*] under the auspices of an extended visit authorization to [*Name of Host Party and, as applicable, the Host Party command or organization*], I am subject to the jurisdiction of United States Federal, State, and local laws, except as provided by treaty, other specific legal authority, or the terms of any diplomatic immunity that I may have been granted. I understand that my acceptance of the Liaison Officer assignment with [*Name of Host Party and, as applicable, the Host Party command or organization*] does not bestow upon me diplomatic or other special privileges.

2. LIAISON OFFICER CONDITIONS OF CERTIFICATION

a. Responsibilities: I understand that my activities shall be limited to the representational responsibilities of my Government and that I am expected to present the views of my Government with regard to the issues that my Government and the U.S. Government have a mutual interest. I shall not perform duties that are reserved by law or regulation to an officer or employee of the U.S. Government.

b. Costs: I understand that all costs associated with my duties as a Liaison Officer shall be the responsibility of my Government, including, but not limited to, travel, office space, clerical services, housing, messing, and medical and dental services.

c. Extensions and Revalidation: I understand that if my Government desires to request an extension or revalidation of my assignment beyond the original dates for which I am certified, a new visit request shall be submitted not later than thirty (30) days prior to the expiration date of the current extended visit authorization.

d. Contact Officer: I understand that when the certification process is completed, a Contact Officer shall be assigned to sponsor me during my visit to the [*Name of applicable Host Party command or organization*]. I further understand that I shall coordinate, through my Contact Officer, all requests for information, visits, and other business that fall under the terms of my certification. I also understand that requests for information that are beyond the terms of my certification shall be made through [the Office of the Defense Attaché, *[Identify Embassy]*, Washington, DC.

e. Other Visits: I understand that visits to facilities for which the purpose does not directly relate to the terms of my certification shall be made through [the Office of the Defense Attaché, [*Identify Embassy*], Washington, DC.

f. Uniform: I understand that I shall wear my national uniform when conducting business at the [*Name of applicable Host Party command or organization*] or other [*Name of Host Party*] facilities, unless otherwise directed. I shall comply with my Parent Government's service uniform regulations.

g. Duty Hours: I understand that my duty hours are Monday through Friday, from [*TIME]* to [*TIME*]. Should I require access to my work area during non-duty hours, I am required to request permission from the Command Security

Officer through my Contact Officer. I further understand that [*IT IS*] [*IT IS NOT*] necessary to assign a U.S. escort officer to me during my non-duty access. Any incremental cost incurred as a result of such non-duty access shall be reimbursed to the U.S. Government.

h. Security:

(1) I understand that access to U.S. Government information shall be limited to that information determined by my Contact Officer to be necessary to fulfill the functions of a Liaison Officer, as described in my assignment description. I also understand that I may not have access to United States Government computer systems, unless the information accessible by the computer is releasable to my Government in accordance with applicable U.S. law, regulations, and policy.

(2) All information to which I may have access during my certification shall be treated as information provided, in confidence, to my Government and shall not be further released or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the U.S. Government.

(3) I shall immediately report to my Contact Officer should I obtain or become knowledgeable of U.S. Government information for which I am not authorized to have access. I further agree that I shall report to my Contact Officer any incidents of my being offered or provided information that I am not authorized to have.

(4) If required, I shall display a security badge on my outer clothing so that it is clearly visible. The U.S. Government shall supply this badge.

i. Compliance: I have been briefed on, fully understand, and shall comply with the terms and conditions of my certification. Failure to comply may result in termination of my certification. I further understand that the termination of my certification does not preclude further disciplinary action in accordance with any applicable Status of Forces Agreement or other international agreements.

j. Definitions of Terms: Terms not defined herein shall have the definitions ascribed to them in the applicable MOA governing my assignment as a Liaison Officer.

3. LIAISON OFFICER TERMS OF CERTIFICATION

a. Contact Officer: [*NAME* OF *CONTACT OFFICER[s]*] has been assigned as my Contact Officer.

b. Certification: I am certified to [*Name of applicable Host Party and, as applicable, the Host Party command or organization*] and shall represent [*Name of Parent Party and, as applicable, the Parent Party command or organization*] to [*Name of Host Party command or organization*], as mutually agreed by the Parties.

c. Travel: I may visit the following locations under the terms of my certification, with the permission of my Contact Officer: [*Insert applicable locations*]

4. LIAISON OFFICER CERTIFICATION OF IN-BRIEFING: *I*, [*NAME OF LIAISON OFFICER*], understand and acknowledge that I have been certified as a Liaison Officer to [*Name of applicable Host Party and, as applicable, the Host Party command or organization*], as agreed upon between [*Name of Parent Party and, as applicable, the Parent Party command or organization*] *and* [*Name of Host Party and, as applicable, the Host Party command or organization*] in accordance with the Memorandum of Agreement (MOA) between the Department of Defense of the United States of America (DoD), as represented by the United States Marine Corps, and the Ministry of Defense [*or appropriate name*] of [*Name of country*] (MOD [*or appropriate acronym*]), as represented by [*Name of foreign military organization or command*], Regarding the Assignment of Liaison Officers. I further acknowledge that I fully understand and have been briefed on: (1) the legal status of my certification; (2) the conditions of my certification; and (3) the terms of my certification. I further acknowledge that I shall comply with the conditions and responsibilities of my certification.

_____
(SIGNATURE OF LIAISON OFFICER)

_____
(TYPED NAME OF LIAISON OFFICER)

_____
(RANK AND/OR TITLE)

_____
(DATE)

_____
(SIGNATURE OF BRIEFER)

_____
(TYPED NAME OF BRIEFER)

_____
(DATE)

FOREIGN DISCLOSURE OFFICER (FDO) APPROVAL MARKING

CMI or CUI information authorized for disclosure to a foreign government(s) shall be marked (in a font size no smaller than 8 pts) on the cover, or the first page of a document or presentation slide inside the cover, or in the footer of the first page of a document where there is no cover:

This briefing/document/item has been approved for disclosure to the government(s) of (insert country name(s) here) (if the document is not approved for release add the statement: This briefing/document/item is not approved for physical or electronic release.) This information is furnished upon the condition that it or knowledge of its possession will not be disclosed to another nation, and that it will not be used for other than the military purpose for which the information was provided without specific authority of the U.S. Marine Corps; that individual or corporate proprietary rights contained within, whether patented or not, will be respected; and that the information will be provided the same degree of security afforded it by the U.S. Department of Defense. Regardless of any declassification markings, this information may not be declassified or downgraded by a foreign recipient without the written approval of the originating U.S. agency.

Note: With the approval of an FDO, the marking should also be inserted below the text of emails containing CMI or CUI sent to foreign government representatives.