C3. CHAPTER 3

TECHNOLOGY TRANSFER AND DISCLOSURE

C3.1. TECHNOLOGY TRANSFER

DoD Directive 2040.2 (reference (u)) requires that the Department of Defense treat defense-related technology as a valuable, limited national security resource and apply export controls to its release. Table C3.T1. summarizes the DoD technology transfer policies implemented through strategic trade licensing, munitions licensing, and the Foreign Military Sales (FMS) processes.

Table C3.T1. DoD Technology Transfer Policies

	DoD Technology Transfer Policies
1	Manage transfers of technology, goods, services, and munitions consistent with United States (U.S.) foreign policy and national security objectives.
2	Control the export of technology, goods, services, and munitions, which could prove detrimental to U.S. security interests.
3	Limit transfers of advanced design and manufacturing know-how to those that support specific national security objectives.
4	Facilitate the sharing of technology only with allies and nations that cooperate in safeguarding the technology and reciprocate in sharing such technology.
5	Seek to strengthen foreign procedures to protect sensitive and defense related technology.
6	Comply with the National Disclosure Policy (NDP) in cases involving the release of classified military information.
7	Ensure that the requirements of DoD Directive 5230.24, DoD Directive 5230.25, and DoD 5200.1-R (references (v), (w), and (x)) are adhered to regarding Controlled Unclassified Information (CUI).
8	Ensure that transfers of munitions and services technology receive special scrutiny, taking into account the importance of arms cooperation with North Atlantic Treaty Organization (NATO) and other close friends and allies, potential third party transfers, and the protection of advanced military operational capabilities.

C3.1.1. Technical Data

C3.1.1.1. Definition of Technical Data. The International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 – 130 (reference (n))) defines technical data as: information, other than software that is required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles including blue prints, drawings, photographs, plans, instructions, and documentation; classified information relating to defense articles and services; information covered by an invention secrecy order; and software, as defined in the 22 CFR part 121.8(f) (reference (n)), directly related to defense articles. Technical data does not include information concerning general scientific, mathematic, or engineering principles commonly taught in schools, colleges and universities, or information in the public domain. Technical data does not include basic marketing information on function, purpose, or general system descriptions of defense articles.

C3.1.1.2. Release Of Technical Data. Releasability of technical data is considered in the same manner as other potentially sensitive parts of the program. In accordance with 22 CFR part 124.2 (reference (n)), the release of technical data is limited to the provision of training in basic

operations and maintenance of defense articles lawfully exported. This specifically excludes the release of technical data for training in support of intermediate and depot level maintenance. Release in support of intermediate and depot level maintenance must be reviewed to ensure that the Technical Data Package (TDP) does not contain information that can be used for design, development, or production of an item. Controlled Unclassified Information (CUI) is exempt from public disclosure under 5 U.S.C. 552 (reference (y)) (Freedom of Information Act) (see paragraph C3.4.1.) and must be reviewed in foreign disclosure channels before release to foreign Governments or international organizations.

C3.1.1.2.1. Release of USG Owned Technical Data. The USG either owns or has the legal right to use defense-related technical data. USG owned TDPs are released under FMS procedures and only in support of a specifically defined, lawful, and authorized USG purpose. The Letter of Offer and Acceptance (LOA) must cover the full cost of preparation, reproduction, and handling of technical data.

C3.1.1.2.2. Release of Privately Owned Technical Data. When private ownership exists, foreign representatives normally request the data through commercial channels. Release is subject to export licensing requirements. If the DoD Components release such information under a Security Assistance program, the data must be properly marked and the owner must authorize release. The Letter of Offer and Acceptance (LOA) must cover the full cost of preparation, reproduction, and handling of technical data.

C3.1.1.3. Requests for TDPs. TDP requests must specify if the TDP is for use in operating and maintaining U.S.-origin defense equipment; for study purposes to determine if a request for production authorization will be submitted; or for production of the defense article or component(s) or follow-on development or improvement of an item of U.S. equipment (or derivations thereof). The LOA must identify the purpose for which the TDP is provided. See Chapter 5, Table C5.T5. for exact note placement and wording.

C3.1.1.4. Sale of TDPs for Operation and Maintenance (O&M). TDPs are sold for O&M only if the Implementing Agency verifies that the article was provided to the purchaser through authorized transfer and there is no other viable means of maintaining the U.S.-origin equipment. The Implementing Agency provides the LOA (or other documentation that validates the authorized transfer of the U.S.-origin equipment) and Table C3.T2. information to the release and disclosure authority for use in making a release determination. If the proposed release involves classified information or CUI, the decision must be approved by a Designated Disclosure Authority appointed pursuant to DoD Directive 5230.11 (reference (h)). A standard note is included in LOAs that contain O&M TDPs. See Chapter 5, Table C5.T5. for the LOA note wording.

Table C3.T2. Data Sheet for TDPs Transferred for Operations and Maintenance

Data Sheet for TDPs Transferred for Operations and Maintenance (O&M)	
1	Nomenclature of hardware, major end item, or component, as applicable
2	Major assemblies or components in TDP having USG patent or other proprietary rights not releasable without prior approval
3	Statement as to whether the TDP requirement would be met by means of pertinent DoD instructions, maintenance manuals, or other similar publications
4	In-country inventory of major end items requiring maintenance support from the requested TDP
5	Current status of DoD maintenance capability (e.g., is there an excess depot level capability at the DoD facility?)
6	Estimated date by which USG repair parts support terminates
7	Security classification of the TDP
8	Identify any classified information or CUI
9	Verification of legal rights to release the TDP for this purpose
10	The DoD Component recommendation on releasing the TDP
11	Attach copy of pertinent correspondence with purchaser

C3.1.1.5. Sale of TDPs for Study or Production. TDPs are offered for study only when the Department of Defense is prepared to release the TDP for production. If an article is in limited supply or if foreign production would adversely impact the U.S. mobilization base, requests for TDPs for study or production are normally denied. The Implementing Agency provides the LOA and Table C3.T3. information to the release and disclosure authority for use in making a release determination. If the proposed release involves classified information or CUI, a Designated Disclosure Authority appointed pursuant to DoD Directive 5230.11 (reference (h)) must approve the decision. Standard notes are included in LOAs that contain TDPs for study or production. See Chapter 5, Table C5.T5. for the wording of these notes.

Table C3.T3. Data Sheet for TDPs Transferred for Study or Production

Data Sheet for TDPs Transferred for Study or Production	
1	Nomenclature of defense article to be studied or produced
2	Quantity to be produced by, and production schedule of, the requesting Government
3	Use of article to be produced, with names of third country purchasers if for third country sale
4	Stock on hand, show separately any quantity beyond approved acquisition objective
5	U.S. and foreign production history for last 5 years
6	Production plans (a) underway, (b) approved, and (c) proposed
7	Estimated date by which USG repair parts support terminates
8	Known U.S. source(s) of supply
9	USG cost of the article
10	Security classification of the TDP and of the article to be produced
11	Other countries authorized to produce the article
12	Anticipated impact of TDP sale on U.S., FMS, or other programs
13	Whether production recipients previously obtained the article and quantities obtained
14	Verification of legal rights to release the TDP for this purpose
15	TDP elements having patent or other proprietary rights not releasable without prior approval
16	Whether TDP requirement could be met by maintenance manuals or other publications
17	The DoD Component recommendation regarding release of the TDP
18	Attach copy of pertinent correspondence with purchaser

C3.1.1.6. Revisioning Services. After TDPs have been approved for transfer, revisioning services can be offered. Revisioning services may appear as a separate line item on the LOA transferring the TDP or they may be offered on a separate LOA. Revisioning services require a unique LOA note shown in Chapter 5, Table C5.T5. If previous TDP transfer notes on the case require updating, the revisioning services LOA must contain the complete provisions required for initial TDP transfer.

C3.1.1.7. Restrictive Markings on TDPs. Implementing Agencies must ensure the TDP includes markings showing the rights of use authorized and not authorized, the security classification, and other restrictions. Each separate part of the technical information including drawings and aperture cards are marked. If individual part marking is not possible, TDP cover information provides the restrictions. DoD Directive 5230.24 and DoD Directive 5230.25 (references (v) and (w)) provide DoD policy and procedures for marking and handling export-controlled technical data that are critical technology. Technical data so marked constitute CUI.

C3.1.1.8. TDPs Related to Defense Articles Manufactured by Watervliet Arsenal. See Chapter 4, paragraph C4.3.10. for information on these items.

C3.1.2. Foreign Manufacture. Foreign manufacture of U.S. equipment benefits the United States when it strengthens friendly defense forces, improves U.S. defense relationships, or enhances interoperability. It may also benefit the United States when it is advantageous to assist in maintaining the purchaser's defense industrial base or in improving general defense capabilities by means of collaborative defense programs. Program implementation can be through an FMS case that provides the purchaser with technical data and authority necessary to operate and maintain or manufacture the defense article. Implementation can also involve an international agreement (such as for cooperative development) or an LOA and complementary international agreement in the form of a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA). (See DoD Directive 5530.3 (reference (aa)).) A program specific MOU or MOA is the preferred method when there is no General Security Agreement with the purchaser. Sample security language for a program specific MOU or MOA is provided at Figure C3.F1.

Figure C3.F1. Sample Text for a Program-Specific Security Agreement

When there is no General Security of Information Agreement or General Security Military Information Agreement with a purchasing government, a program specific security agreement will contain the provisions described below, at a minimum. The agreement must be approved by the Office of the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (DUSD(TSP&NDP))) prior to discussion with the purchasing government. Any modification to the text during negotiation must be approved by the DUSD(TSP&NDP). Once the terms set forth in the agreement are agreed upon, the DUSD(TSP&NDP) shall sign or delegate authority to sign the agreement.

1. The first paragraph shall contain a reference to the pertinent Letter of Offer and Acceptance, citing the Case Designator, and indicate that the agreement takes precedence. For example: This security agreement between the Department of Defense of the United States of America and the Ministry of Defense of the Government of [insert the country] (hereafter, "the Parties") establishes the terms and conditions by which classified information and material related to the [insert system] to be sold to the Government of [insert the country] under Letter of Offer and Acceptance [insert Case Designator] will be protected. In the case of any difference in interpretation between the terms of Letter of Offer and Acceptance [insert Case Designator] and this Agreement, the terms of this Agreement will govern. The Parties hereby agree as follows:

2. Definitions:

   a. Information - Knowledge in any form (i.e., in oral, visual or material form).

   b. Classified Information - Information that has been determined to require protection in the interests of national security and is marked with a classification designation by the country that originated the information (e.g., Top Secret, Secret, Confidential, or Restricted).

   c. Material - Tangible matter, such as documents, equipment, photographs, magnetic tapes, computer disks, or other tangible matter that my contain information.

   d. Facility - Physical location, such as a building or compound.

   e. Disclose/Disclosure - Providing of information in any form (i.e., oral, visual, or material).

   f. Release - Disclosure of information in material form (e.g., documentary form).

3. Classified information and material shall be transferred through official government channels or through other channels that may be agreed upon in writing by the responsible security officials of the Parties. When a transfer of classified information or material is executed, a Transportation Plan shall be prepared to describe security requirements and arrangements for each segment of the transfer, from the point of origin to the ultimate destination.

4. Each Party shall take all lawful steps available to it to ensure that classified information and material provided or generated pursuant in connection with the sale of the (cite system) shall be protected from compromise or further disclosure unless such disclosure is authorized by the Party that provided the information or material. Accordingly, each Party shall:

   a. The recipient Party will not disclose or release or authorize the disclosure or release of the information or material to any government, person, firm, organization, or other entity of a third country, or to any firm, organization or entity that is owned or controlled by a third country person or entity, without the prior written consent of the Party that provided the information or material.

Figure C3.F1. Sample Text for a Program-Specific Security Agreement (cont)

b. The recipient Party shall not use or permit the use of the classified information or material for any purpose other that for which it was provided pursuant to Letter of Offer and Acceptance [insert Case Designator] without the prior written consent of the Party that provided the information or material.

c. The recipient Party will provide security protection for the classified information or material in a manner that is no less stringent than the protection provided to its own classified information and material of an equivalent security classification level.

5. Prior to the disclosure or release of any classified information or material provided or generated under Letter of Offer and Acceptance [insert Case Designator] to a person or a facility within its territory, consistent with paragraph 4.a., above, the recipient Party shall:

a. Ensure that any facility (governmental or commercial) to which the information or material may be provided has the capability to protect the information or material and the responsible person at the facility has executed a written contractual arrangement under which the person agrees to provide such protection.

b. Ensure that all persons who will be authorized to have access to the information or material have been determined to be qualified for access to classified information, have an official need for such access, and have been informed of their responsibilities for protecting the information or material.

c. Appoint a person at each facility that will have access to the classified information or material who will be responsible for ensuring the proper protection of the information or material.

d. Conduct periodic inspections of all facilities that will have access to the information or material and ensure that the information or material is properly protected.

6. Each Party shall report to the other Party any loss or compromise, or potential loss or compromise, of classified information or material provided or generated under Letter of Offer and Acceptance [insert Case Designator].

7. Any visit by representatives of either Party to the territory of the other Party related to Letter of Offer and Acceptance [insert Case Designator] shall be submitted through government channels in compliance with the visit procedures of the country that will host the visit. Visitors shall be required to protect any classified information or material disclosed or released during the visit in compliance with this Agreement.

8. Each Party shall accept visits by security officials of the other Party, when mutually convenient, to review the requirements set forth in this Agreement.

9. This agreement shall remain in force as long as classified information or material provided or generated under Letter of Offer and Acceptance [insert Case Designator] remains in the possession of the Government of [insert Country].

C3.2. MISSILE TECHNOLOGY CONTROL REGIME

C3.2.1. Missile Technology Control Regime (MTCR) Definition. The MTCR is an informal international political arrangement designed to control the proliferation of rocket and unmanned air vehicle (UAV) systems (and their associated equipment and technology) capable of delivering weapons of mass destruction. It was formed in 1987 and currently includes 33 member countries. Regime controls are applicable to all items on the MTCR annex to include all items listed in 22 CFR part 121.16 (reference (n)). The MTCR Annex Handbook is published by the DoS (http://www.mtcr.info/).

C3.2.2. MTCR Screening Process. Although the regime is a political commitment rather than a treaty with international legal obligation, many countries, including the United States, have passed laws restricting the export of MTCR-controlled items (Arms Export Control Act (AECA), Chapter 7 (reference (c))). The Department of State (DoS), the Department of Commerce (DoC), and the Department of Defense all have a role in regulating the export of MTCR-controlled items from the United States. The Department of Defense identifies MTCR-controlled items that purchasers have requested via FMS.

C3.2.2.1. The System Program Office (SPO), Program Manager (PM), or equivalent performs a technical review of each LOA, as early in the LOA development process as practical. Possible MTCR-controlled items contained in the LOA or envisioned to be part of the associated program are identified. To ensure technical reviews are standardized, reviewers must complete a Defense Security Cooperation Agency (DSCA)-approved Missile Technology Proliferation Course, or have equivalent experience in MTCR and Ballistic Missile Proliferation. Implementing Agencies maintain a roster of personnel trained and/or knowledgeable on MTCR controls.

C3.2.2.2. Implementing Agencies screen all LOAs for MTCR-controlled items. The LOA transmittal memorandum to DSCA must contain a statement that a qualified individual accomplished an MTCR review. If MTCR items ARE NOT identified in the review, this is stated in the LOA transmittal memorandum. If MTCR-controlled items ARE identified in the LOA, the following procedures are used.

C3.2.2.2.1. The reviewer transmits a list of the MTCR-controlled items to the Implementing Agency MTCR point of contact (POC) at the earliest opportunity to ensure minimal delays in the LOA processing time. This list includes: the case identifier; a general case description identifying major associated systems; the Military Articles and Services List (MASL) number of each MTCR-controlled item; the nomenclature of each item; and a detailed description of each item including the manufacturer.

C3.2.2.2.2. The reviewer must report the compounds listed in Item 4 of the MTCR Annex if they are to be exported in bulk as an input for a manufacturing process, or in any other manner or form that might support the creation of a propellant for a missile or a UAV. However, the reviewer is NOT to report Item 4 explosive compounds if they are molded or poured into a form that precludes their use as rocket propellant (e.g., as a bursting, propelling, or gas-generating charge in a shell, cartridge, squib, or actuator).

C3.2.2.2.3. The reviewer is NOT to report as a possible MTCR-controlled item any common type munition fuse, even though all such fuses meet the criteria of Item 2.A.1.f. in the

MTCR Annex (i.e., "weapon or warhead safing, arming, fusing and firing mechanisms…"). If the fuse in question is an unusual type, a rough equivalent of which is not likely to be found in most foreign arsenals, or if the fuse uses sophisticated means to determine burst height (e.g., radar), the reviewer should report it.

C3.2.2.2.4. The Implementing Agency MTCR POC verifies the list and forwards it via memorandum to DSCA (Programs Directorate/Weapons Division). The memorandum should be submitted electronically to mtcr@dsca.mil. The name, telephone and fax number, and e-mail address of the Implementing Agency MTCR POC are included.

C3.2.2.2.5. DSCA (Programs Directorate/Weapons Division) reviews and forwards the memorandum to the DoS, Deputy Director, Office of Chemical, Biological, and Missile Threat Reduction, Bureau of International Security and Nonproliferation (ISN/MTR), for review and approval.

C3.2.2.2.6. DoS (ISN/MTR) coordinates the possible transfer of the MTCR-controlled items. This process is accomplished in advance of final LOA development to avoid delays.

C3.3. COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (C4ISR)

C3.3.1. C4ISR Definition. C4ISR encompasses systems, procedures, and techniques used to collect and disseminate information. It includes intelligence collection and dissemination networks, command and control networks, and systems that provide the common operational/ tactical picture. It also includes information assurance products and services, as well as communications standards that support the secure exchange of information by C4ISR systems. Under the C4ISR umbrella, systems exchange digital, voice, and video data to appropriate levels of command. The two key classified aspects of C4ISR systems are access to secure networks controlled by Information Security (INFOSEC) products and services, and the classified data resident in the C4ISR networks. See CJCSI 6510.06 (reference (ap)) for information on the release of U.S. INFOSEC products (e.g., Communications Security (COMSEC), cryptographic algorithms, cryptographic key material, security infrastructure, etc.) to foreign purchasers. Transfers of U.S. C4ISR capabilities to countries and international organizations must support a U.S. Combatant Commander's (COCOM) interoperability requirements or otherwise clearly benefit U.S. policy objectives (e.g., telemetry test data transmissions for FMS aircraft transfers). A purchaser's desire to be interoperable with the United States is insufficient justification for release. Prior to physically receiving any U.S. INFOSEC products or services associated with a secure C4ISR system, the purchaser must negotiate and sign a Communication Interoperability and Security Memorandum of Agreement (CISMOA) or other INFOSEC agreement (e.g., COMSEC MOU, INFOSEC Equipment Agreement) with the COCOM. A purchaser must obtain approval from the supporting COCOM for access to classified U.S. C4ISR and INFOSEC prior to submitting a Letter of Request (LOR) for C4ISR. See Chapter 5 for more information on processing LORs for C4ISR equipment and services. Pre-LOR coordination activities will take place between the requesting foreign purchaser (via SCO in country or Embassy in U.S.) and DSCA (Programs Directorate) (see section C3.3.4).

C3.3.2. C4ISR Release Process.

C3.3.2.1. Release of Classified Military Information. Interoperable systems that exchange classified military information are subject to a releasability review and approval as defined in National Disclosure Policy (NDP-1). In addition to classified system hardware and software information, all data flowing between foreign and secure U.S. C4ISR systems are classified. Approvals for release of U.S. classified data flowing over secure coalition networks are required before issuance of LOA and/or P&A data. (see section C3.6.).

C3.3.2.2. INFOSEC Release. The release process for INFOSEC products is defined in CJCSI 6510.06 (reference (ap)). With two exceptions (see paragraph C3.3.2.3. and C3.3.2.4. below) all INFOSEC releases to non-NATO (excluding Australia and New Zealand) nations are limited to specific quantities in support of a specific interoperability requirement.

C3.3.2.3. Global Positioning System/Precise Positioning System (GPS/PPS) and Identification Friend or Foe (IFF) Mode IV Releases. All INFOSEC products require release before being offered on an FMS case. GPS/PPS and IFF Mode IV releases are not tied to a specific quantity or platform. Once these devices are approved for release, the purchaser may obtain these products through National Security Agency-authorized channels.

C3.3.2.4. Bilateral INFOSEC Agreement Signature. A bilateral agreement (e.g., CISMOA or COMSEC MOU, INFOSEC Equipment Agreement) must be in place in order for a purchaser to receive INFOSEC products or services associated with a C4ISR system.

C3.3.3. C4ISR Oversight/Steering Group. The C4ISR Oversight/Steering Group consists of representatives from DSCA, OSD (NII), Chairman, Joint Chiefs of Staff, the COCOM, Implementing Agencies, and NSA. C4ISR Oversight/Steering Group meetings, chaired by OSD NII International Affairs, are called annually, or as needed, to address policy, operational, or acquisition issues for Phases 1 and 2 C4ISR programs. This group gathers policy-related information from implemented Phases 1 and 2 FMS cases to ensure current programs are in compliance with existing policy or whether existing policy needs to be changed to address new circumstances.

C3.3.4. C4ISR Responsibilities. Table C3.T4. lists organizations and their C4ISR responsibilities.

Table C3.T4. C4ISR Responsibilities

Organization	Responsibility
Security Cooperation Organization	• Informs host country of the requirement for COCOM sponsorship of requests for INFOSEC-enabled C4ISR systems • Promotes the C4ISR three-phased approach (3PA)(see paragraph C3.3.5. for more information), to assist the country with planning and budgeting for secure interoperability with U.S. C4ISR systems and capabilities • Coordinates pre-LOR C4ISR requirements with DSCA (Programs Directorate through Operations Directorate) • Forwards LOR after pre-coordination to Implementing Agency
Purchaser	• Signs bilateral CISMOA or other binding INFOSEC agreement • Coordinates with SCO on pre-LOR C4ISR requirements • Submits C4ISR LOR for each phase of the C4ISR 3PA to SCO who then forwards to Implementing Agency that has been determined during the pre-LOR consultations with DSCA

Organization	Responsibility
	• Submits LOR for a dedicated INFOSEC facility, and staffing by two U.S. accredited COMSEC custodians to Implementing Agency (see C3.3.5.)
U.S. Combatant Commander (COCOM)	• Establishes interoperability requirement for specific C4ISR capabilities requiring INFOSEC products and services • Initiates CJCSI 6510.06 (reference (ap)) INFOSEC release process • Participates in CONOPS development in Phase 1 • Following delegation from the Chairman, Joint Chiefs of Staff, negotiates and signs the CISMOA or other appropriate bilateral INFOSEC agreement governing the transfer of INFOSEC products and services to non-NATO (excluding Australia and New Zealand) nations • Serves as member of C4ISR Oversight/Steering Group
DSCA	• DSCA (Operations and Programs Directorate) reviews C4ISR pre-LOR requirements in coordination with NSA and COCOM, and, as appropriate, assigns the lead Implementing Agency • Monitors planning activities • Serves as Executive Secretary of the C4ISR Oversight/Steering Group • Provides input to and review of the C4ISR planning process and Phases 1 and 2 deliverables
Implementing Agencies	• Receive and review C4ISR LORs after pre-LOR review by DSCA • Obtain DSCA (Operations Directorate) approval before processing LOR • Obtain input and coordinate LOA Data with all activities participating in Phases 1 and 2 • Generate Price and Availability (P&A) data and/or FMS case • Serve as members of the C4ISR Oversight/Steering Group
National Security Agency (NSA)	• Identifies the appropriate INFOSEC solution to satisfy COCOM validated interoperability requirements • Delegates authority through the Chairman, Joint Chiefs of Staff to the COCOM to negotiate the COMSEC portion of the CISMOA, or to negotiate INFOSEC Equipment Agreements • Generates FMS case for foreign purchase of U.S. INFOSEC products and services; under limited circumstances, provides written authority to MILDEPs to include specific INFOSEC products and services on Military Department FMS cases (see National COMSEC Instruction (NACSI) 6001 (reference (am)) • Serves as member of the C4ISR Oversight/Steering Group
Chairman, Joint Chiefs of Staff	• Validates COCOM interoperability requirements associated with the requests for U.S. INFOSEC products and services • Delegates final authority to COCOM to negotiate and conclude the CISMOA • Serves as member of the C4ISR Oversight/Steering Group
Office of the Secretary of Defense (OSD) Networks and Information Integration (NII)	• Provides input to and review of Phases 1 and 2 products • Chairs the C4ISR Oversight/Steering Group

C3.3.5. C4ISR Planning Process - Three-Phased Approach (3PA). To the greatest extent possible, C4ISR foreign requirements are addressed from a joint service perspective. Before a C4ISR LOR is submitted, pre-coordination with DSCA (Operations and Programs Directorates), the respective COCOM, potential Implementing Agencies, the SCO, and the foreign purchaser is recommended. Through this pre-LOR coordination, DSCA determines whether the COCOM supports the transfer, identifies releasability challenges, and designates the lead Implementing Agency and, where applicable, supporting Implementing Agencies in advance of receiving the

C4ISR LOR (see C5.1.4.3.5). DoD encourages the use of a 3PA to plan C4ISR programs, as outlined below. Separate LORs are normally submitted for each individual phase of the 3PA.

C3.3.5.1. Phase 1. Before submitting an LOR for the acquisition of a C4ISR system, purchasers are encouraged to submit an LOR for C4ISR planning that explores the intended Concept of Operations (CONOPS) and develops an overarching C4ISR architecture that ensures efficient, interoperable, and economical technical solutions that enhance interoperability with U.S. forces. The deliverables of Phase 1 include a CONOPS, a risk assessment of the purchaser's current communications architecture, and development of a notional high-level architecture based on both COCOM and purchaser requirements. If the purchaser opts not to have an FMS case for C4ISR planning (e.g., Phase 1), then the FMS case to support the C4ISR system sale should include provisions to address interoperability, CONOPS, and C4ISR architecture development. The lead Implementing Agency, in concert with the supporting Implementing Agencies, will present to the C4ISR Oversight/Steering Group the joint program management concept for executing Phase 1 approximately 90 days after LOA signature.

C3.3.5.2. Phase 2. Phase 2 provides a Procurement Plan that is a "total package" of options and recommendations with associated costs, schedules, and risk impacts to the purchaser. It is generated within the purchaser's budget and funding constraints, using performance engineering assessments, and includes analysis of alternatives of select specific hardware/software solutions, risk analyses and trade-offs, and infrastructural assessment. Other tasks include definition of information exchange requirements, refinement of high-level architecture, and initiation of C4ISR training. Due to the joint nature of these programs, DSCA will assign a lead Implementing Agency to coordinate and integrate other Implementing Agency input into the P&A data/FMS case. If required, the lead Implementing Agency, in concert with the supporting Implementing Agencies, presents the Procurement Plan to the C4ISR Oversight/Steering Group for review.

C3.3.5.3. Phase 3. Phase 3 implements the procurement strategy through FMS, direct commercial sales (DCS), and/or cooperative programs. Implementing Agencies may only execute sales of INFOSEC articles and related services for which NSA has provided written FMS sales authority to the Implementing Agency, in accordance with NACSI 6001 (reference (am)).

C3.3.6. INFOSEC LOAs. The Director, National Security Agency, (DIRNSA) is the National Manager for INFOSEC products to include both external Communications Security (COMSEC) equipment and embedded cryptographic modules. The Implementing Agency for COMSEC and embedded cryptographic modules is determined by the Acquisition Manager of a particular device. DIRNSA may allow some NSA managed INFOSEC materiel to be included on other Implementing Agency managed LOAs due to urgent operational requirements, end of fiscal year funding issues, etc. Requests for exceptions to allow NSA-managed INFOSEC materiel on other Implementing Agency LOAs will not be granted due to the lack of an existing NSA LOA or to avoid the Small Case Management Line. Special Purpose INFOSEC equipment ("S" Type COMSEC) shall be provided to Non-NATO Nations on NSA-managed FMS cases only. Requests to allow "S" Type COMSEC equipment on other Implementing Agency LOAs will not be granted.

C3.3.6.1. INFOSEC Validation/Authorization. All Implementing Agencies must request DIRNSA determination as to whether INFOSEC equipment and embedded cryptographic modules are releasable, and whether the releasable equipment/modules can be included on an LOA written by an Implementing Agency other than NSA. DIRNSA authorization is required even when the Implementing Agency is responsible for the acquisition of the INFOSEC equipment and embedded cryptographic modules. Requests must include a copy of the purchaser's LOR, nomenclature of the INFOSEC and/or embedded cryptographic modules, quantities, and identify the weapon system or platform in which the INFOSEC equipment will be integrated. DIRNSA will provide a written response to the Implementing Agency within 30 days of the request. Some responses may include special instructions for INFOSEC materiel that requires special handling.

C3.3.6.2. Classification of INFOSEC. The association of a specific INFOSEC product with a foreign government may be classified; however, classifying the entire FMS case will be avoided, when possible. See Chapter 5, C5.4.11. for more information on classified FMS cases.

C3.3.7. INFOSEC Accounts, Facilities, and Custodians. C4ISR purchasers may be required to establish a dedicated INFOSEC account and purchase an INFOSEC facility manned by two U.S. accredited INFOSEC custodians. The COCOM, during the negotiation phase of the CISMOA with the purchaser, determines if the INFOSEC account requirement applies to a purchaser. NSA and the COCOM may assign additional duties to INFOSEC custodians.

C3.3.8. Electronic Warfare (EW) Systems and EW Integrated Reprogramming Database (EWIRDB)

C3.3.8.1. Definition. EW Systems (e.g., radar warning receivers and jammers) are designed to deny or counteract the enemy's use of electromagnetic (EM) emitters, e.g., radar, communications, guidance, detection, and control devices. The sale of an EW capability involves the transfer of the EW system hardware, firmware, and software. The software typically includes a mission data file (MDF) or library which contains information/data related to EM emitters. The EWIRDB is the primary DoD source for technical parametric performance data on EM emitters and is used to program/reprogram the MDF to correctly identify emitters by their EM characteristics. Prior to offering an LOA to the FMS customer that includes an EW system, the FMS Implementing Agency must review all EW system components to verify the system, to include the MDF, has been approved for release and certified in writing by the appropriate DoD authorities (i.e. National Security Agency (NSA), National Air and Space Intelligence Center (NASIC), Defense Intelligence Agency (DIA), and applicable program offices). If an EW system is not certified in writing prior to sale, the FMS purchaser must be advised and the FMS Implementing Agency must ensure a plan is in place to obtain data protection certification from the NSA prior to delivery. Delivery cannot take place without this certification. An exception to the data protection certification requirement is when the FMS customer uses its own technical parametric performance data instead of DoD data.

C3.3.8.2. FMS EWIRDB Types. The FMS EWIRDB is used to create the MDF or library for EW systems. There are two types of FMS EWIRDB, Direct and Indirect. A Direct FMS EWIRDB is delivered directly to the FMS customer and provides data required for an In-Country Reprogramming (ICR) capability for the EW system. An Indirect FMS EWIRDB is delivered to the U.S. reprogramming facility that will develop the MDF for the requesting

country's EW system. Both Direct and Indirect EWIRDBs must go through the release processes described below prior to the FMS sale.

C3.3.8.3. EW Release Process. An LOR advisory should be issued to NSA and the applicable MILDEPs by DSCA (Operations Directorate) when an LOR is received for an EW system that will be used on a country's weapon system for the first time. This advisory will notify the EW community of the pending request so that the evaluation process can begin. It is critical that the evaluation process be initiated as soon as possible due to the amount of time required to complete the process.

C3.3.8.4. Release of Classified Military Information. EW systems that use classified military information are subject to a releasability review and approval as defined in the National Disclosure Policy (NDP-1). In addition to possible classified system hardware and software, the system MDF may include classified data. Approvals for release of U.S. classified data are required before an LOA can be offered to a purchaser.

C3.3.8.5. EW System Requirements. All U.S. origin systems that are being considered for export require NSA Data Protection Certification prior to handling classified data. In addition, Anti-Tamper (AT) review by the DoD AT Executive Agent (ATEA) is required as noted in C3.4. of the SAMM. It is the responsibility of the Implementing Agency (IA) and the vendor to ensure the system is NSA certified prior to loading classified information. A copy of the accreditation should be provided to DSCA (Programs Directorate) by the IA. During LOA development, the IA should identify a plan that incorporates all the required acquisition milestones. Such a plan will ensure delivery of a weapon system platform that provides all the required capabilities, to include EW. The IA should also incorporate any leadtime or costs into the FMS LOA required for NSA certification, in the event an EW system is offered but not yet certified.

C3.3.8.6. FMS EWIRDB Release in Principle. Prior to offering an LOA for FMS EWIRDB support, there must be an approved and valid Release in Principle (RIP) in place for the use of the Direct or Indirect FMS EWIRDB. The FMS EWIRDB RIP is issued by NSA for a particular country on a specific weapon system platform, and is not related to a COMSEC RIP. Once the IA Program Office or vendor determines there is an FMS EWIRDB requirement, a request for a RIP should be submitted to the appropriate IA EW point of contact listed in Table C3.T5. The IA will designate a point of contact for receipt of these requirements to ensure consistency in the submissions to the DoD authorities. The request for a RIP will be submitted to the DoD disclosure authorities (Table C3.T5.). At a minimum, these requests will identify the requesting country, platform, type of database (Direct/Indirect) and EW system nomenclature, if known. Once the RIP is granted, an LOA for FMS EWIRDB support can be offered to the purchaser. The IA should enter comments in DSAMS case remarks stating that an EW RIP has been granted, citing the approving agency, date of grant, and point of contact.

C3.3.8.7. FMS EWIRDB Release in Specific. Upon acceptance by the customer of an LOA for an EW system with FMS EWIRDB support, the IA EW point of contact will coordinate with the country to determine the desired data to be incorporated into the FMS EWIRDB. This information, along with the identified recipient country, platform, type of database (Direct/Indirect) and EW system will be used by the EW points of contact at the applicable IA to develop a request for a Release in Specific (RIS). The RIS will be submitted to the DoD

disclosure authorities for approval. If approved, the RIS will authorize the EWIRDB executive agent, the National Air and Space Intelligence Center (NASIC) to begin the development of an FMS EWIRDB for a particular country, platform, and EW system as funded by an FMS LOA. Table C3.T5. EW Responsibilities. Table C3.T5. lists organizations and their EW responsibilities.

Table C3.T5. EW Responsibilities

Organization	Responsibility
DSCA	• Prepares LOR Advisory for potential sale of EW system • Reviews LOA prior to offer to ensure appropriate reviews have been accomplished
Implementing Agencies	• Provides copy of LOR to DSCA with details on what EW system will be proposed for potential platform sale, to be used for LOR advisory • Determine if proposed EW system has been certified by NSA for handling of classified data • Incorporate required EW costs and program schedule impacts into LOA; advise purchaser of certification status and potential schedule risks and impacts • Reviews LOA and verifies appropriate reviews have been accomplished prior to being offered to customer
Implementing Agency EW Points of Contact • Air Force (Deputy Under Secretary of the Air Force for International Affairs Regional Weapons Division) • (SAF/IARW) • Army (Deputy Assistant Secretary of the Army for Defense Exports and Cooperation) (SAAL-NI) • Navy (Navy International Programs Office Strategic Planning Directorate) (Navy IPO-03)	• Process any required disclosure requests for applicable classified military information • Work with program office and vendor to develop technical documentation required for evaluation of EW systems data protection • Evaluate requirement to determine if RIP has been granted for a particular system. If not, submit request for RIP to DIA, NSA and SIGCOM for approval/authorization • Upon LOA signature work with purchaser as applicable to identify data base requirements and submit request for RIS to DIA, NSA and SIGCOM for approval/authorization • Validate that LOA is written appropriately to incorporate specific EW verbiage.
Defense Intelligence Agency (DIA)	• Review and process Service requests for EW system RIP and RIS

Organization	Responsibility
National Security Agency (NSA)	• Review and process Service requests for EW system RIP and RIS • Review and provide guidance for data protection certification for EW systems
National SIGINT Committee (SIGCOM)	• Review and process Service requests for EW system RIP and RIS
Purchaser	• Upon LOA signature participate in dialog with IA FMS offices to identify required data to be included in EW data base

C3.3.8.8. LOA Requirements. All LOAs that offer EW systems and/or data base support must clearly identify, in the LOA notes, the nomenclature of the EW system components, the type of data base support being provided and the platforms associated with the EW system and/or data base support. The LOA notes must clearly state if an EW system is not certified prior to the LOA being offered.

C3.4. ANTI-TAMPER (AT) POLICY COMPLIANCE

The U.S. Government reserves the right to incorporate AT technologies and methodologies in weapons systems and components offered under the Security Assistance Program, which contain Critical Program Information (CPI). Prior to proposal for transfer of materiel containing CPI, the Implementing Agency will coordinate with the DoD Anti-Tamper Executive Agent (DoD ATEA) to ensure sensitive technologies or program information is defended against unlawful exploitation or loss. The DoD ATEA is located at Suite 1500, 1500 Wilson Blvd, Arlington, Virginia 22209. Implementing agencies shall certify compliance with AT requirements on the LOA transmittal memorandum forwarded to DSCA for LOA processing.

C3.5. DISCLOSURE OF CLASSIFIED MILITARY INFORMATION

C3.5.1. Disclosure of Classified Military Information Policy. DoD Directive 5230.11 (reference (h)) implements National Disclosure Policy (NDP-1). It is U.S. national and DoD policy that classified military information is a national security asset that shall be protected. It can be shared with foreign Governments only when there is a clearly defined benefit to the United States, when authorized by officials designated under DoD Directive 5230.11 (reference (h)), and when all DoD Directive 5230.11 (reference (h)) requirements are met.

C3.5.2. Disclosure Authorities. Under the terms of NDP-1, the National Disclosure Policy Committee (NDPC) is the central authority for formulating, promulgating, administering, and monitoring NDP-1. The Secretary of Defense or the Deputy Secretary of Defense are the only officials who may grant unilateral exceptions to the National Disclosure Policy. However, in most cases, exceptions to policy are granted or denied by the NDPC. Under DoD Directive 5230.11 (reference (h)), the Secretary of Defense has delegated disclosure authority to the Secretaries of the Military Departments (MILDEPs) and other DoD officials whose decisions must be in compliance with NDP-1. They are required to appoint a Principal Disclosure Authority (PDA) at component headquarters level to oversee the disclosure process and a

Designated Disclosure Authority (DDA) at subordinate command and agency levels to oversee disclosure decisions at their level when disclosure authority is delegated. It is the PDA or DDA who is authorized to make disclosure decisions, unless authority is otherwise delegated in a Delegation of Disclosure Authority Letter (DDL).

C3.5.3. Disclosure Decisions.

C3.5.3.1. Disclosure of classified information relating to defense articles and services is evaluated on a case-by-case basis in accordance with NDP-1, DoD Directive 5230.11 (reference (h)), and MILDEP regulations. Specifically designated foreign disclosure officials in the MILDEPs and defense agencies (see paragraph C3.3.2) must authorize disclosure of information originated by or for those departments and agencies. The Implementing Agency uses the resulting disclosure determination to implement approved transfers of classified information.

C3.5.3.2. Disclosure authorizations for classified information are recorded in the National Disclosure Policy System (NDPS), Foreign Visit System (FVS), and Foreign Disclosure System (FDS), which are part of the DoD Security Policy Automation Network (SPAN). The Technology Protection System (TPS) (also part of SPAN) is used to process export license applications.

C3.5.3.3. The SPAN operates both a classified and a separate unclassified network. The classified network supports coordination among DoD activities on export control, international arms control and cooperation subjects in addition to foreign disclosure decisions. Foreign embassies within the National Capital Region are able to process international visit and requests for documentary information through the unclassified network.

C3.5.4. False Impressions. U.S. policy is to avoid creating false impressions of its readiness to make available classified military materiel, technology, or information. Much military hardware is unclassified; however its operation and maintenance or related training may involve sensitive classified information. Some classified information (e.g., Sensitive Compartmented Information (SCI), COMSEC information, etc.) may require approval outside of the Department of Defense and the NDPC. Therefore, initial planning to include the release of unclassified Price and Availability (P&A) Data with foreign governments and international organizations concerning programs which might involve the eventual disclosure of classified military information may be conducted only if such action is coordinated with a designated disclosure official from the originating organization and it is explicitly understood and acknowledged that no U.S. commitment to furnish such classified information or materiel is intended or implied until disclosure has been approved. Accordingly, proposals to foreign governments or international organizations which result from either U.S. or combined (U.S. and proposed recipient) initial planning, and which will lead to the eventual disclosure of classified military information, must be authorized in advance by designated disclosure officials in the departments and agencies originating the information or by the NDPC.

C3.5.5. Visits, Assignments, and Exchanges of Foreign Nationals. Many disclosures of classified information occur as a result of visual demonstrations or verbal exchanges during meetings or visits. DoD Directive 5230.20 (reference (ab)) contains standard procedures concerning visits, assignments, and exchanges of foreign nationals to the Department of Defense and to DoD contractor facilities over which the DoD Components have security responsibility. Approval of a classified visit is a disclosure decision. With few exceptions, visits and

assignments requiring access to classified material are processed through the DoD FVS of the SPAN. One exception is for visits by students under Security Assistance-sponsored training programs where the DD Form 2285, "Invitational Travel Orders (ITO)" (see Chapter 10, Figures C10.F3. and C10.F4.) provides the necessary security information. Visits are categorized as one-time, recurring, or extended visit authorizations.

C3.5.5.1. One-Time Visit Requests. Approval of a one-time visit request permits a single, short-term (normally less than 30 days) visit for a specified purpose.

C3.5.5.2. Recurring Visit Requests. A recurring visit authorization permits intermittent visits over a specified period of time for a Government-approved license, contract or agreement, or other program when the information to be released has been defined and approved for release in advance by the USG.

C3.5.5.3. Extended Visit Requests. An extended visit permits a single visit for an extended period of time (beyond 30 days) for a foreign Government contract or joint program (e.g., joint venture, representative to a joint or multinational program), or for a liaison officer, exchange officer, or cooperative program person under authorized international agreements. Before any commitment is made to assign a liaison officer to a cleared defense contractor facility in support of the sale of defense articles or services, the extended visit shall be coordinated and agreed to with the contractor and the supporting Defense Security Service (DSS) office, in order to fix responsibility for security oversight. The specific terms of the assignment, including security responsibility, shall be set forth in the supporting contract.

C3.5.6. National Industrial Security Program (NISP). U.S. security depends on the proper safeguarding of classified information released to industry. The NISP assures safeguarding of classified information released during all phases of the contracting, licensing and grant process to cleared U.S. contractor facilities. The NISP also applies to all classified information not released under a contract, license certificate, or grant and to Foreign Government Information (FGI) furnished to contractors that requires protection in the interest of national security. DoD 5220.22-R (reference (ac)) provides NISP policies, practices, and procedures used by the Department of Defense to ensure maximum uniformity and effectiveness in its application throughout industry. DoD 5220.22-M (reference (m)) contains detailed security requirements for U.S. contractors' use in safeguarding classified information. The NISPOM is applied to industry by management's execution of the DoD Security Agreement (DD Form 441), and by direct reference in the "Security Requirements" clause in the contract. The Defense Industrial Security Clearance Office (DISCO) verifies the eligibility of industry personnel to access classified defense information.

C3.5.7. U.S. Contracts with Foreign Firms. Implementing Agencies may award (or permit a contractor to award) a classified contract to a foreign contractor provided the classified information is releasable to the Government of the foreign contractor under NDP-1. The Government of the foreign contractor must also have a security agreement or other security arrangement with the United States wherein it agrees to protect the classified information released to it. Implementing Agency responsibilities are contained in DoD 5220.22-R (reference (ac)). Foreign disclosure implications are identified by the program office and resolved by the supporting DDA, prior to any announcements that could lead to foreign involvement. Classified

information must be requested and transferred through Government channels in compliance with the DoD Component documentary request procedures.

C3.5.8. Contracts Requiring Overseas Deliveries. When an Implementing Agency places a contract with a cleared U.S. contractor for delivery of classified information or materiel to a foreign Government, the Implementing Agency is responsible for delivery. See Chapter 7 for more information regarding transportation of classified information.

C3.5.9. Release of Classified FMS Case Planning Information.

C3.5.9.1. Tentative Security Assistance Plans and Programs. Classified planning information for budget and future years may be released to a foreign Government or international organization to the extent it is necessary for participation in the security assistance planning process; it is necessary for development of related defense plans; the purchaser can maintain security precautions; and the purchaser uses the information only for the intended purposes. If the release involves classified information or CUI, the release must be approved by the supporting DDA. Classified dollar levels of proposed programs may be released only with permission of the Director, DSCA, and DoS concurrence. U.S. officials releasing information under this paragraph ensure that the recipient understands that the release does not constitute a commitment by the United States.

C3.5.9.2. FMS Agreements. Once approved, classified information regarding the quantity and projected delivery schedules for articles and services in FMS agreements may be released to facilitate appropriate planning by the recipient, subject to assurance by the recipient that it shall maintain adequate security precautions and shall use the information only for the purposes for which provided.

C3.5.9.3. Procedures for Release. Release of classified information under subparagraphs C3.5.9.1. and C3.5.9.2. is subject to the provisions of DoD Directive 5230.11 and DoD 5200.1-R (references (h) and (x)). Release is made only to purchaser Government officials who require the information in their official capacity.

C3.6. RELEASE OF INFORMATION

C3.6.1. Freedom of Information Act (FOIA). Records containing security assistance-related information, including LOAs and FMS procurement contracts, are released in accordance with the Freedom of Information Act, 5 U.S.C. 552 (reference (y)) as implemented in DoD 5400.7-R (reference (ad)), DoD Instruction 5400.10 (reference (ae)), and DoD 5200.1-R (reference (x)).

C3.6.1.1. Any request under the FOIA for an LOA or FMS procurement contract should be referred to the appropriate counsel of the DoD Component for action. Final decisions to withhold or release, in whole or in part, LOAs already accepted or in preparation shall be coordinated with DSCA (Office of the General Counsel).

C3.6.1.2. Under FOIA exemption (b)(4) (reference (y)), commercial or financial information provided to the USG in confidence by a person (including a foreign Government or a domestic or foreign business) may be exempt from disclosure to the public if it is the type of information that is NOT released by the originator; if disclosure is likely to cause substantial competitive harm to the originator; if disclosure is likely to impair the ability of the USG to obtain necessary commercial or financial information in the future; or if disclosure is likely to

impair some other legitimate USG interest. Such information is to be marked "For Official Use Only" in compliance with DoD 5400.7-R (reference (ad)). If the DoD Component determines that it may be required to disclose commercial information obtained in confidence from a person, corporation, or foreign Government, it shall notify the submitter of the information in accordance with DoD 5400.7-R (reference (ad)), and Executive Order 12600 (reference (af)).

C3.6.1.3. Under FOIA exemption (b)(3) (reference (y)) and 10 U.S.C. 130c (reference (ag), effective October 1, 2000, information provided by, made available by, or produced in cooperation with, a foreign Government or international organization may be withheld from release.

C3.6.2. Release of Unclassified Information. Except as provided in subparagraph C3.1.1.2., unclassified information pertaining to systems for which the purchaser has been authorized release may be provided by the USG to the purchaser country or international organization as appropriate for purposes related to security assistance.

C3.6.3. In-Country Release Approval. Once a disclosure decision has been made in accordance with paragraph C3.5.3., the Chief of the U.S. Diplomatic Mission must approve in-country release of all security assistance information to a purchaser.

C3.6.4. Release of Foreign Government Information. Information provided by a foreign Government (both classified and unclassified) in confidence, is held in confidence when the foreign country expects it to be treated as such. Similar information produced by the USG as a result of a joint arrangement with a purchaser is also held in confidence. DoD 5200.1-R (reference (x)) provides instructions for protecting such information.

C3.6.4.1. Classification of foreign Government information is in accordance with DoD 5200.1-R (reference (x)). Foreign Government classification decisions shall be honored and under no circumstances modified without the express written consent of the Government that provided the information.

C3.6.4.2. Requests for mandatory review for the declassification of foreign Government information are processed in accordance with DoD 5200.1-R (reference (x)).

C3.7. EXPORT LICENSE AND CUSTOMS CLEARANCE

C3.7.1. International Traffic in Arms Regulations (ITAR) Requirements. DoS policies and procedures for the permanent export of items on the U.S. Munitions List (USML), purchased under the FMS program, are set forth in the ITAR (reference (n)). The ITAR can be found at the website: http://www.pmdtc.org/reference.htm. Export of USML items, including certain services and technical information, generally requires a license unless it is done via FMS. The Defense Technology Security Administration (DTSA) vets license applications through the Department of Defense and other departments. This is done using the TPS. TPS allows all agencies, which might have an interest in the technology in question to review the proposed export and to restrict its terms and conditions, or recommend denial of license, if warranted. TPS includes search and historical retrieval capabilities.

C3.7.2. International Traffic in Arms Regulations (ITAR) Exemptions. There are many exemptions to the licensing requirements in reference (n). Some are self-executing by the contractor who is to use them, and normally are based on prior authorizations. Other

exemptions, such as the exemption in 22 CFR 125.4(b)(1) (reference (n)) may be requested or directed by the DoD Component. Only a Principal or a Designated Disclosure Authority has the authority to exercise certain of these exemptions in compliance with the NISPOM (reference (m)).

C3.7.3. DoD-Sponsored Shipments of FMS Materiel.

C3.7.3.1. Export License Requirements for DoD-Sponsored Shipments. An export license is not required when FMS materiel is moved through the Defense Transportation System (DTS) unless the purchaser takes custody of the materiel in the United States. A DSP Form 94 is required pursuant to ITAR, Part 126.6(c)(6)(ii) (reference (n)). When classified material is involved, a Transportation Plan is required in accordance with ITAR, Part 126.6(c)(6)(iii) (reference (n)).

C3.7.3.2. U.S. Customs Clearance Requirements for DoD-Sponsored Shipments. A Shipper's Export Declaration (SED) (U.S. DoC Form 7525-V) may be required when FMS materiel is moved through DTS. If a continental U.S. (CONUS)-located shipping activity offers FMS shipment directly to commercial air carriers for lift to a purchaser's country, it may be necessary for the shipper to prepare a SED to enable the materiel to depart CONUS. (Item 16 in the SED must contain "M"s to identify the materiel as FMS exports. The Census Bureau maintains a web page (http://www.census.gov/foreign-trade/www/correct.way.html) and customer assistance phone number to assist shippers with SED preparation.)

C3.7.3.3. Overseas Customs Clearance Requirements for DoD-Sponsored Shipments. The purchaser is responsible for obtaining overseas customs clearances and for all actions and costs associated with customs clearances for deliveries of FMS materiel using DTS to a purchaser's port of discharge (including delivery to third countries).

C3.7.3.4. Reporting of FMS Export Shipments for DoD-Sponsored Shipments. All USG and DoD-sponsored shipments of FMS export materiel moving overseas within DTS are reported monthly to the Foreign Trade Division, Bureau of Census, DoC, by the MILDEP or Implementing Agency sponsoring the sale. The Census Bureau Shipment Report (CBSR) assures compliance with conditions under which exemptions are granted and satisfies the export data requirements of the U.S. DoC.

C3.7.4. Purchaser-Sponsored Shipments of FMS Materiel.

C3.7.4.1. Export License Requirements for Purchaser-Sponsored Shipments. An export license is not required when FMS materiel is transferred; however, ITAR Form DSP-94 (Figure C3.F2.) must be used to export these shipments. A DSP-94 must be accompanied by a signed and implemented LOA. Table C7.T3. outlines responsibilities for FMS purchasers and their freight forwarders. To use a DSP-94, a freight forwarder must: be registered with the DoS, Directorate of Defense Trade Controls; file a letter with the Directorate of Defense Trade Controls from the foreign embassy or Government appointing them as a forwarding agent for that Government's shipments; file a statement with the Directorate of Defense Trade Controls assuming full responsibility for compliance with reference (n); and have a security clearance issued by DSS if it is to handle classified consignments. If a foreign purchaser acts as its own freight forwarder, it must register with the Directorate of Defense Trade Controls and file a statement that it shall comply with reference (n). If the materiel involves classified articles or

data, a cleared courier or escort and a Transportation Plan is required. See 22 CFR 126.6 (reference (n)) for requirements.

C3.7.4.2. U.S. Customs Clearance Requirements for Purchaser-Sponsored Shipments. The purchaser must obtain customs clearances for FMS materiel exported from the United States by its freight forwarder or other non-DTS means. The purchaser's representative or freight forwarder prepares the SED. SEDs must be filed with and authenticated by the District Director of Customs at the port of exit. Laws and regulations concerning export declarations are found on the reverse side of Department of Commerce Form 7525-V, and in 22 CFR 123.9, 123.22, 123.25, and 126.6 (reference (n)). A SED is required for the following types of shipments.

C3.7.4.2.1. All exports of materiel made through or by the FMS purchaser's freight forwarder or other designated agent.

C3.7.4.2.2. Pilot pick-up of materiel by the purchaser's military aircraft or purchaser-chartered civilian aircraft at a CONUS DoD-controlled aerial port of embarkation (APOE).

C3.7.4.2.3. Export by purchaser-owned or chartered ocean vessel, or by FMS country-procured space aboard commercial vessel picking up cargo at CONUS DoD-controlled water port of embarkation (WPOE).

C3.7.4.3. Overseas Customs Clearance Requirements for Purchaser-Sponsored Shipments. The purchaser is responsible for obtaining overseas customs clearances and for all actions and costs associated with customs clearances for deliveries of FMS materiel using commercial means to a purchaser's port of discharge (including delivery to third countries).

C3.7.4.4. Reporting of Non-DTS Exports for Purchaser-Sponsored Shipments. All exports of FMS materiel from the United States shall be reported to the U.S. DoC as required by current Federal statutes or regulations.

C3.7.4.5. Purchaser-Sponsored Shipments of Classified FMS Materiel. If a purchasing country proposes to take possession of classified defense articles identified in 22 CFR Part 121 (reference (n)), purchased under the FMS program within the United States, it must obtain an export authorization (e.g., see 22 CFR Part 125 (reference (n)) regarding licensing of technical data) from the DoS in accordance with the ITAR. Classified defense articles are only licensed using a Form DSP-85 (Figure C3.F3.), an approved manufacturing or technical assistance agreement, or an exemption.

C3.7.4.5.1. Transportation Plan for Purchaser-Sponsored Shipments. The applicable LOA must contain the requirement for a Transportation Plan, describe the specific responsibilities for preparing the Transportation Plan, and provide a generic description of the transfer arrangements and nationality of freight forwarders and carriers to be used, all of which shall be consistent with DoD 5200.1-R (reference (x)) and DoD 5220.22-M (reference (m)). While the transfer procedures may be included in the LOA when Government-owned transportation is used, a Transportation Plan is always required for the use of any commercial carrier. The consignment shall be accompanied by a courier or escort who possesses a personal security clearance at least at the classification level of the consignment. The security office that supports the FMS Case Manager provides assistance and ensures that the arrangements are in compliance with DoD policy. FMS shipments are not released until the supporting security

office verifies that the transfer arrangements meet DoD standards. The FMS Case Manager provides the DSS advance copies of all Transportation Plans that involve U.S. defense contractors, freight forwarders, or commercial carriers. These plans are provided for information purposes and are to be used by the addressees as a means to clarify their role and responsibilities in the transfer process. The Transportation Plan must be completed and approved before delivery of the item. A copy of the plan must be included in the case file. Figure C3.F4. summarizes the Transportation Plan requirements. Figure C3.F5. is a sample format for the Transportation Plan as provided in the International Program Security Handbook (reference (ah)).

C3.7.4.5.2. Foreign Government Representative. Classified material may be released only to a person who has been designated by the purchasing Government in writing as its Designated Government Representative (DGR) or as its transfer agent (e.g., freight forwarder) that is used for onward movement to the point where custody of the shipment is assumed by the Government's DGR. A freight forwarder or commercial carrier cannot act as the purchasing Government's DGR; they are only transfer agents. The Military Assistance Program Address Directory (MAPAD) (reference (t)) may be consulted for the verification of freight forwarders that have been approved to handle classified shipments. However, the shipping activity verifies security clearances of U.S. cleared freight forwarders and carriers and their personnel with the DSS prior to releasing a shipment to them. The identity of the transfer agent, carrier, and DGR is included in the Transportation Plan or in the Notice of Consignment for individual shipments (see Figure C3.F4.). The identity of the person who signs for the shipment may also be contained in the shipping activity's Notice of Availability, but must be in the Transportation Plan or Notice of Consignment. Each entity that has custody of a classified shipment shall be required to sign a receipt for the shipment, regardless of the security classification, and a copy of each receipt is returned to the shipping activity.

C3.7.4.6. Purchaser-Sponsored Shipments of Commercially-Purchased Materiel.

C3.7.4.6.1. Export License and Customs Clearance Requirements for Purchaser-Sponsored Shipments of Commercially-Purchased Materiel. Commercial exports made by a foreign Government or its freight forwarder require an export license and SED. The U.S. vendors involved in the direct commercial sale (DCS) must obtain the export license (i.e., a DSP-5 for permanent exports or a DSP-73 for temporary exports).

C3.7.4.6.2. Classified Shipments under Direct Commercial Sales (DCS) for Purchaser-Sponsored Shipments of Commercially-Purchased Materiel. Classified shipments resulting from DCS must comply with the same security standards that apply to FMS contracts. Prior to consummation of a DCS contract that results in the shipment of classified material, contractors must consult with the purchasing Government and the DSS Cognizant Security Office to obtain approval of the contractor-prepared Transportation Plan. In the event the defense contractor is unable to make suitable arrangements for shipment of classified material procured under a DCS contract, the contractor should advise the purchaser to make appropriate DTS shipment arrangements under an FMS LOA.

C3.7.4.6.3. FMS Credit Financed Direct Commercial Contracts. DSCA approval of Foreign Military Financing (FMF) for a DCS contract does not relieve the exporter from

obtaining required export licenses, nor imply automatic USG approval of such licenses when requested.

C3.7.5. Temporary Imports.

C3.7.5.1. Temporary Import of Unclassified Defense Articles. A Temporary Import License, ITAR Form DSP-61 (Figure C3.F6.) is required for the import and re-export from the United States of unclassified defense articles that are not associated with an FMS Repair and Return or similar program pursuant to an executed FMS case. The Transportation Plan that is prepared for the initial sale will include instructions and requirements for imports for Repair and Return. See 22 CFR part 123.4 (reference (n)) for more information.

C3.7.5.2. Temporary Import of Offshore Procurements. Materiel procured outside of the United States under USG and DoD procurement actions for the FMS program must be imported and exported under a DSP-61 if it passes through the United States en route to the purchasing country unless an exception under 22 CFR part 123.4 (reference (n)) applies (there are additional exceptions for Canada and Mexico under 22 CFR parts 123.19 and 126.5 (reference (n)). The DSP-61, filed by the purchaser or its agent, is required whether the materiel is imported or exported intact or is incorporated into another defense article that is subsequently exported to the purchasing country.

C3.7.5.3. Temporary Import of Defense Articles for Repair. Articles temporarily imported to the United States for overhaul, repair, modification, etc., under an LOA are exempt from the DSP-61 requirement. When it is anticipated that articles will be returned to the United States for overhaul, repair, or modification, the import requirements shall be included in the Transportation Plan or LOA for the original sale. The purchaser or its agent is responsible for filing documentation with U.S. Customs upon entry of Repair and Return materiel into the United States. This documentation (e.g., Customs Form 3461, 7512, etc.) must contain the statement,

> "This shipment is being imported in accordance with and under the authority of 22 CFR part 123.4(a)(subsection____)"

and include a complete list and description of the defense articles being imported. The description includes quantity and value in U.S. dollars. When the materiel is subsequently re-exported, the purchaser or its agent must submit a SED to the District Director of U.S. Customs that cross-references to the import documentation. The SED or an attachment must also contain the statement, "22 CFR (section____) and 22 CFR part 120.1(c) applicable." Shipments moved via the DTS do not require import or export processing with U.S. Customs. Implementing Agencies preparing LOAs for Repair and Return programs include a note (see Chapter 5, Table C5.T5.) indicating the requirement for the foreign country to report imports and exports made under the LOA to U.S. Customs.

C3.7.5.4. Temporary Imports of Defense Articles Without Subsequent Export of the Same Article. Under 22 CFR part 123.4(b) (reference (n)), a license is not required for the temporary import (but not the subsequent export) of unclassified defense articles that are to be incorporated into another article; or modified, enhanced, upgraded, altered, improved or serviced in any other manner that changes the basic performance or productivity of the article. A DSP-5 is required for the re-export of these enhanced defense articles unless FMS exceptions apply.

C3.7.6. Permanent Imports. The Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives (BATFE), pursuant to the AECA and implementing federal regulations, regulates the permanent import of defense articles, as listed in the United States Munitions Import List (based on the USML). Imports of defense articles into the United States require an approved permit issued by BATFE.

C3.7.7. Contractor Proposals and Presentations. Policy and procedures for DoS approval regarding sales proposals or presentations of Significant Military Equipment (SME) are in 22 CFR part 126.8 reference (n). These requirements do not apply to SME that has been approved for sale under FMS.

C3.7.7.1. Export License Requirement. If marketing efforts involve the disclosure of technical data or temporary export of defense articles, the contractor must obtain the appropriate export license.

C3.7.7.2. Prior Approval for Contractor Presentations and Proposals. DoS approval must be obtained before any marketing efforts for sales that meet ALL of the following criteria: SME valued at $14 million or more; end-use by foreign armed forces other than NATO countries, Australia, New Zealand, or Japan; export of any defense article or the furnishing abroad of any defense service including technical data; and identical SME has not been previously licensed for permanent export or approved for sale under the FMS program. This prior approval permits the contractor to conduct unclassified discussions and propose a sale of a specific item of SME to a particular country.

C3.7.7.3. Advance Notification for Contractor Presentations and Proposals. When the identical equipment meets the first three conditions in subparagraph C3.5.7.2. and has not been previously licensed for permanent export or approved for sale under the FMS program to any foreign country, the contractor must notify the DoS in writing at least 30 days in advance of the proposal or presentation.

C3.7.7.4. Prior Approval for Manufacturing Licensing Agreements (MLA) and Technical Assistance Agreements (TAA). Prior approval must be obtained for all proposals to enter a MLA or TAA with a foreign country for the production or assembly of SME. An MLA or TAA is not required during the period in which the FMS case and implementing USG FMS contracts and subcontracts are in effect. Under 22 CFR part 126.6 (reference (n)), the LOA and the implementing contracts serve as the authorization for the transfers without a license.

Figure C3.F2. Department of State Form, DSP-94, Authority to Export Defense Articles and Defense Services Sold Under the Foreign Military Sales Program

OMB APPROVAL NO. 1405-0051
EXPIRATION DATE: NOVEMBER 30, 1991
ESTIMATED BURDEN: 30 MINUTES

UNITED STATES OF AMERICA
DEPARTMENT OF STATE

AUTHORITY TO EXPORT DEFENSE ARTICLES AND DEFENSE SERVICES SOLD UNDER THE FOREIGN MILITARY SALES PROGRAM

This form, when properly executed and accompanied by an authenticated Department of Defense Offer and Acceptance (DD Form 1513), constitutes authority under section 126.6 of the International traffic in Arms Regulations (ITAR) to export the defense articles and defense services listed thereon. This form may be used in lieu of a Department of State export license to export defense articles and services sold by the Department of Defense under the Foreign Military Sales (FMS) program. This export authority is valid for 2 years from the date shown in item 12 below.

The Department of State may, without prior notice to the exporter, deny, revoke, suspend, or amend this authority consistent with ITAR section 126.7.

Willful violation of the ITAR, making an untrue statement of a material fact, or omission of a material fact required to be stated on this form are subject to prosecution and, upon conviction, fines up to $100,000 or up to 2 years' imprisonment, or both. (Section 38(c), Arms Export Control Act; section 127.3, ITAR.)

1. PM/DTC Applicant Code	2. Country of Ultimate Destination/Purchaser	3. Port of Exit from U.S.
4. Applicant's Name, Address, ZIP Code, Tel. No.	5. Foreign Military Sales Case Identifier	6. Date of FMS Case Implementation
	7. Total Value of Defense Articles and Defense Services of Original FMS Case $ _____	
	8. Only the unshipped balance, valued at $_____, of this FMS case is covered by this DSP-94. Previous shipments of this FMS case were covered by a Form DSP-94 dated _____ and/or Department of State license No. _____	

9. Form DSP-94 constitutes an amendment to the value and/or quantity of defense articles and services authorized under this FMS case as shown in the attached-amended DD Form 1513. Yes ☐ No ☐

10. If exporter is a freight forwarder acting on behalf of a foreign government or diplomatic mission, provide the name, address, and telephone number of the foreign official in the U.S. familiar with this FMS case.

11. U.S. Munitions List Categories (see section 121.1 of the ITAR). Please check the appropriate categories to indicate the types of defense articles and/or defense services included on this FMS case:

I. _____	VI. _____	XI. _____	XVI. _____	XXI. _____
II. _____	VII. _____	XII. _____	XVII. _____	
III. _____	VIII. _____	XIII. _____	XVIII. _____	
IV. _____	IX. _____	XIV. _____	XIX. _____	
V. _____	X. _____	XV. _____	XX. _____	

12. Exporter's Statement

I, _____, hereby exercise the authority to effect the export described above; warrant the truth of all statements made herein; and acknowledge, understand, and will comply with the provisions of Title 22 CFR Parts 120-130 and any conditions and limitations imposed.

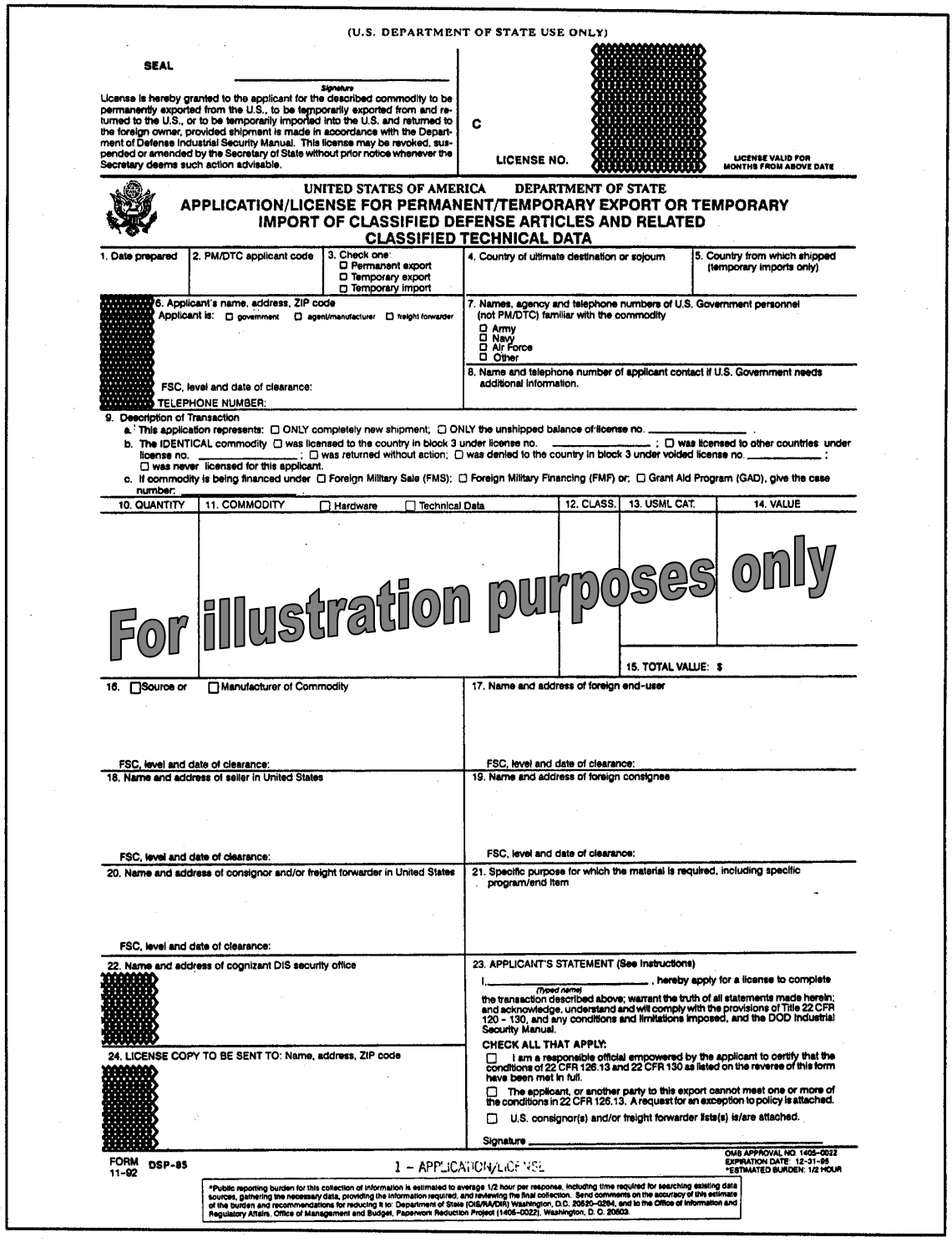
Signature _____ Date _____

(Authority valid for 24 months from above date.)

1 - AUTHORITY TO EXPORT

FORM DSP-94
12-91

Figure C3.F3. Department of State Form, DSP-85, Application-License for Permanent-Temporary Export or Temporary Import of Classified Defense Articles and Related Classified Technical Data .



(U.S. DEPARTMENT OF STATE USE ONLY)

SEAL

Signature

License is hereby granted to the applicant for the described commodity to be permanently exported from the U.S., to be temporarily exported from and returned to the U.S., or to be temporarily imported into the U.S. and returned to the foreign owner, provided shipment is made in accordance with the Department of Defense Industrial Security Manual. This license may be revoked, suspended or amended by the Secretary of State without prior notice whenever the Secretary deems such action advisable.

C

LICENSE NO.

LICENSE VALID FOR MONTHS FROM ABOVE DATE

UNITED STATES OF AMERICA DEPARTMENT OF STATE

APPLICATION/LICENSE FOR PERMANENT/TEMPORARY EXPORT OR TEMPORARY IMPORT OF CLASSIFIED DEFENSE ARTICLES AND RELATED CLASSIFIED TECHNICAL DATA

1. Date prepared	2. PM/DTC applicant code	3. Check one: ☐ Permanent export ☐ Temporary export ☐ Temporary import	4. Country of ultimate destination or sojourn	5. Country from which shipped (temporary imports only)

6. Applicant's name, address, ZIP code
Applicant is: ☐ government ☐ agent/manufacturer ☐ freight forwarder

FSC, level and date of clearance:

TELEPHONE NUMBER:

7. Names, agency and telephone numbers of U.S. Government personnel (not PM/DTC) familiar with the commodity
☐ Army
☐ Navy
☐ Air Force
☐ Other

8. Name and telephone number of applicant contact if U.S. Government needs additional information.

9. Description of Transaction

a. This application represents: ☐ ONLY completely new shipment; ☐ ONLY the unshipped balance of license no. _____ .

b. The IDENTICAL commodity ☐ was licensed to the country in block 3 under license no. _____ ; ☐ was licensed to other countries under license no. _____ ; ☐ was returned without action; ☐ was denied to the country in block 3 under voided license no. _____ ; ☐ was never licensed for this applicant.

c. If commodity is being financed under ☐ Foreign Military Sale (FMS); ☐ Foreign Military Financing (FMF) or; ☐ Grant Aid Program (GAD), give the case number: _____ .

10. QUANTITY	11. COMMODITY ☐ Hardware ☐ Technical Data	12. CLASS.	13. USML CAT.	14. VALUE

15. TOTAL VALUE: $

16. ☐ Source or ☐ Manufacturer of Commodity

FSC, level and date of clearance:

17. Name and address of foreign end-user

FSC, level and date of clearance:

18. Name and address of seller in United States

FSC, level and date of clearance:

19. Name and address of foreign consignee

FSC, level and date of clearance:

20. Name and address of consignor and/or freight forwarder in United States

FSC, level and date of clearance:

21. Specific purpose for which the material is required, including specific program/end item

22. Name and address of cognizant DIS security office

24. LICENSE COPY TO BE SENT TO: Name, address, ZIP code

23. APPLICANT'S STATEMENT (See Instructions)

I, _____ (Typed name) , hereby apply for a license to complete the transaction described above; warrant the truth of all statements made herein; and acknowledge, understand and will comply with the provisions of Title 22 CFR 120 - 130, and any conditions and limitations imposed, and the DOD Industrial Security Manual.

CHECK ALL THAT APPLY:

☐ I am a responsible official empowered by the applicant to certify that the conditions of 22 CFR 126.13 and 22 CFR 130 as listed on the reverse of this form have been met in full.

☐ The applicant, or another party to this export cannot meet one or more of the conditions in 22 CFR 126.13. A request for an exception to policy is attached.

☐ U.S. consignor(s) and/or freight forwarder lists(s) is/are attached.

Signature _____

FORM DSP-85 11-92

1 - APPLICATION/LICENSE

OMB APPROVAL NO. 1405-0022
EXPIRATION DATE: 12-31-95
*ESTIMATED BURDEN: 1/2 HOUR

*Public reporting burden for this collection of information is estimated to average 1/2 hour per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (DIS/RA/DIR) Washington, D.C. 20520-0294, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Paperwork Reduction Project (1405-0022), Washington, D. C. 20503.

Figure C3.F4. Transportation Plan Requirements

Transportation Plan Requirements

DoD 5200.1-R, "Information Security Program," (reference (x)) and DoD 5100.76-M, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives," (reference (ai)), require that the transmission instructions or the requirement for an approved Transportation Plan be incorporated into the security requirements of the LOA when the foreign purchaser proposes to take delivery and custody of classified material in the United States and use its own facilities and transportation for forward shipment to its territory. The requirement for this plan shall be included with any contract, agreement, LOA, or other arrangement involving the release of classified material to foreign entities. The Transportation Plan is developed by the DoD Component that prepares the LOA in coordination with the purchasing government. It is to be submitted to, and approved by, the applicable DoD Component security authorities and a copy will be provided to DSS when freight forwarders or commercial carriers are involved, when consignment is directed to a commercial firm, or if the consignment emanates from a U.S. contractor location. The FMS Case Manager and supporting security office must coordinate with DSS and other Government security and Customs authorities to ensure that the proper security arrangements are made under such circumstances. As a minimum, the Transportation Plan shall include the following provisions:

a. A description of the classified material together with a brief narrative as to where and under what circumstances transfer of custody occurs;

b. Identification, by name or title, of the DGR of the foreign recipient Government or international organization who will receive and assume responsibility for the materiel and U.S. DGR who will verify the security arrangements and approve the release of the consignment. In case of classified material, the person(s) so identified must be cleared for access to the level of the classified material to be shipped;

c. Identification and specific location of delivery points, stops or layover points, transfer points, and the identification of a point of contact and alternate at each location (including telephone and cell phone numbers and email address) who will provide assistance;

d. Identification of commercial carriers and freight forwarders or transportation agents who are involved in the process, the extent of their involvement, and, as applicable, security clearance status verified by DSS;

e. Identification of any storage or processing facilities to be used and, relative thereto, certification that such facilities are authorized by competent Government authority to receive or process the level of classified material to be shipped and a primary and alternate point of contact, including telephone and cell phone numbers and email address, who can provide assistance;

f. When classified material is involved, the identification, by name or title, of couriers and escorts to be used and details as to their responsibilities and security clearance status;

g. Description of shipping methods to be used, together with the identification of carriers (foreign and domestic). For classified material, see DoD 5200.1-R (reference (x)), Chapter 8, and for classified sensitive materiels, see DoD 5100.76-M (reference (ai)), Chapter 7;

h. In those cases when it is anticipated that the U.S. classified material or parts thereof may be returned to the U.S. for repair, service, modification, or other reasons, the plan must require that shipment shall be via a carrier of U.S. or recipient Government registry, handled only by security-cleared authorized personnel, and that the applicable DoD Component (for FMS) or DSS (for commercial sales) is given advance notification of estimated time and place of arrival and is consulted concerning inland shipment, as well as the identification of a point of contact and an alternate, with telephone and cell phone numbers and email address, who will provide assistance;

Figure C3.F4. Transportation Plan Requirements (cont)

i. The plan shall require the DGR of the recipient Government or international organization to examine shipping documents upon receipt of the classified material in its own territory and advise the responsible DoD Component in the case of FMS, or DSS in the case of commercial sales, if the materiel has been transferred enroute to any carrier not authorized by the Transportation Plan or other circumstances that deviated from the procedures in the plan;

j. The recipient Government or international organization also is required to inform the responsible DoD Component or the DSS promptly and fully of any known or suspected compromise of U.S. classified material while such materiel is in its custody or under its cognizance during shipment;

k. The plan shall include each segment of the route from the point of origin to the ultimate destination, including all border crossings and actions required at border crossings, together with the identification of a point of contact and alternate at each location, including telephone and cell phone numbers and email address, who can provide assistance. If overnight stops are required, security arrangements for each stopping point must be specified, to include contingency stopovers as necessary; and

l. The plan will include a requirement for transportation instructions with respect to material that is to be returned to the United States for modification, upgrade, or repair.

Figure C3.F5. Sample Transportation Plan for the Transfer of Classified Material

AUTHORIZATION: [Insert FMS Case Designator, Export License Number, Authorization Letter, or ITAR Exemption]

A. PURPOSE. This Transportation Plan describes procedures for the transfer by commercial carrier of the [insert the name and military nomenclature (if applicable) of the defense article or technical data] between the United States and [insert recipient country] as authorized by [insert the FMS Case Designator, License Number, Authorization Letter, or Exemption, as applicable. If an ITAR Exemption is cited, identify the underlying FMS Case, License, etc.].

[Guidance: If there is to be a single shipment under the FMS case or license, the format and requirements of this basic plan should be used. If there are to be recurring shipments, this format should be used as a generic plan to describe the requirements and terms of reference that are standard to all recurring shipments (such as packaging, procedures for handling searches by port security and Customs officials); the details for each shipment will appear in an annex to the basic plan, using the format for a Notice of Consignment at the annex. If this plan is to be a generic plan that provides the standard requirements and general terms of reference for recurring shipments, with the individual consignments described in detail in an attachment, that fact should be so stated here. Also see section B, below, and the annex, "Notice of Classified Consignment," which is to be used for the shipment of each individual consignment. A Transportation Plan will be used for consignments only up to the Secret classification level; Top Secret material must always be transferred via Government courier.]

B. DESCRIPTION OF CONSIGNMENT. [Provide a specific, detailed description of the material to be transferred (list end items, parts, sub-assemblies, software, test equipment, technical documents, etc., together with nomenclature (when applicable) and serial numbers). No classified information should appear in the description. The description of items of material to be transferred under this plan may be appended to the plan as an attachment when the plan is used for a single shipment, or included in a Notice of Classified Consignment (see annex) for recurring shipments.

C. IDENTIFICATION OF RESPONSIBLE GOVERNMENT AND/OR COMPANY REPRESENTATIVES [This section will identify by name and/or title (when a specific named person is not appropriate) and organization, the Government and/or company security or licensing officials who will participate in the activities related to the transfer, together with the nature of their responsibilities (e.g., actions to verify shipment against the license, verify security arrangements, coordinate with airport security and Customs officials). The list will include depot or company security and licensing officials and the Designated Government Representatives (DGRs) of the dispatching country who will verify the adequacy of the arrangements for the transfer and approve release of the consignment, and those of the receiving country who will sign receipts for, and assume final security responsibility for the classified consignment. Mailing addresses, telephone, telefax, and cell phone numbers (both for business and non-business hours) and e-mail addresses are to be listed for each country's representatives. (Freight forwarders and other commercial agents shall not be designated to act as a Government representative; they are transfer agents.) This information also may be included as an attachment or in the "Notice of Classified Consignment" when there are to be recurrent shipments and the information will be different for each shipment.]

D. IDENTIFICATION OF COMMERCIAL ENTITIES TO BE INVOLVED IN EACH SHIPMENT. [Identify fully all commercial entities, such as freight forwarders, customs brokers, and commercial carriers (trucking companies, airlines, surface ships, etc.), including DTS-contracted carriers, that will be involved. Include the level of facility security clearance and storage capability of each entity's facility. For each listed entity, include names of points of contact and their alternates and their addresses, telephone, telefax, and cell phone numbers (for business and non-business hours), e-mail addresses, and the specific functions that named persons will perform (a position may be identified when it is not appropriate to cite a person by name). This information must include the name of the captain of the aircraft or vessel or other on-board representative who has been briefed on the shipment and is to provide assistance. If there will be recurring shipments and the information will vary for each shipment, the details will be placed in the "Notice of Classified Consignment".]

Figure C3.F5. Sample Transportation Plan for the Transfer of Classified Material (cont)

E. PACKAGING THE CONSIGNMENT. [Fully describe how the material is to be packaged. Packaging requirements will conform to the national security rules of the dispatching organization. The requirements for dispatch documents, inventories, seals, receipts, storage, and security containers will be explained. Any unique requirement of the sending and receiving Governments also should be stated. When there are to be recurrent shipments and the details would be different; the specific requirements will be placed in the Notice of Consignment.]

F. ROUTING OF THE CONSIGNMENT. [Briefly identify in the basic paragraph the route to be taken, including the point of origin (e.g., identity of a military depot, contractor facility, etc.), any locations other than the destination where there will be stops or layovers, or the transfer of custody will occur, (e.g. names and addresses of freight forwarder facilities, ports, railheads, airports, airline terminal, etc.), and the final destination. Then describe the specific activities at each individual location for which handling and/or security oversight arrangements must be undertaken (e.g., the movement of a shipment from a Constant Surveillance Service truck to the hold of an aircraft), as indicated in subparagraphs 1 through 5, below. The establishment of these arrangements will require advance coordination between the shipper and airline or surface transport officials, and local security officials (e.g., airport and airline security and Customs) at the point of origin, at stops or layovers, and transfer points, and similar coordination at the destination by officials of the receiving Government. The courier or escort must be provided with a written description of the arrangements that have been made, to include the identities of the points of contact and alternates (see section G, below), and the courier's or escort's responsibilities for each occurrence (e.g., observing the loading or unloading of a shipment to ensure maintenance of security). Also describe any special security arrangements that will be required because of the unique nature of a transfer, stop or layover, or processing point (e.g., an airport freight terminal or port receiving station), and the specific duties of persons who will be responsible for each action. For example, if a programmed layover is required, arrangements must be made for security storage of the consignment; this might entail arrangements with local Government officials. Contingency stopover locations must be anticipated and arrangements made for such situations (e.g., an unexpected landing in a third country). Provide the specific information described below regarding the specific activities that are necessary at each location that is listed. For recurring shipments, any information that is different for a specific shipment may appear in the "Notice of Classified Consignment" for each shipment.

1. Procedures and responsibility for notifying the DGRs and the carrier and port security officials, and Customs in each country of the arrangements and schedule for the shipment (e.g., date, time, carrier, flight number, port, etc.).

2. Procedures and responsibility for verifying and overseeing the loading and sealing/locking the consignments on the carrier. Describe procedures at the loading points and any transfer points, to include verifying tally records, surveillance responsibilities, and witnessing of the counting and loading arrangements.

3. Procedures for arranging accessibility by the courier to the consignment en route (e.g., layovers, stops, diversions, etc.), such as priority disembarking from an aircraft at a stop. These procedures must be arranged in coordination with any freight forwarder/transfer agent and port and carrier security authorities.

4. Procedures for unloading at the destination, to include identification of a pre-arranged representative of the dispatching Government in country who will provide assistance (if applicable) and the recipient Government's DGR, and procedures for change of custody, and receipt arrangements. If there are to be shipments to various locations and/or the arrangements are to be different for each shipment, this section may be very brief and the "Notice of Classified Consignment" annex will be used for the details.

5. Emergency communication procedures. List telephone, telefax, and cell phone numbers (for business and non-business hours) and email addresses for dispatching and recipient Government points of contact to be notified at each location (including stopovers) in the event of emergency. For recurring shipments, this information will be placed in the "Notice of Classified Consignment" annex.]

Figure C3.F5. Sample Transportation Plan for the Transfer of Classified Material (cont)

G. COURIERS/ESCORTS. [This section will describe the procedures for the use of couriers or escorts from the point of origin to the ultimate destination. When couriers or escorts are to be used, they must be identified by name and title, organization, and passport number and/or other secondary identification, and include the identity of a dispatching company or Government official who may be contacted to verify the identity of the courier/escort. Documentation required by or to be provided to the courier or escort will be described here. The section will include procedures for ensuring that the courier or escort is aware of the rules necessary to comply with Customs and security requirements. Provide in this section the procedures for handling Customs searches, and identify points of contact and alternates (the names and telephone, telefax and cell phone numbers (for business and non-business hours) and email addresses of Government officials who may be called upon for assistance, together with the identity of the Customs and port security officials with whom prior arrangements have been made).]

[Guidance: A courier (term used for a person who is carrying the material in his or her possession) or escort (term used for a person who is responsible for overseeing the security of material that is shipped as freight and stowed in the carrier) must accompany the consignment unless the commercial carrier possesses a Facility Security Clearance and agrees in the contract to provide a courier or escort who has the necessary personnel security clearance. Couriers and escorts may not be third-party persons (i.e., contract couriers). They must be cleared at the classification level of the material to be shipped and be briefed on their security responsibilities. Briefings of couriers or escorts will be tailored to the mode of transfer (e.g. commercial air, ships, truck, rail etc.). The courier must be provided the identity, by name, of the specific person who is designated as the receiving Government's DGR, as well as the means by which such person will be identified (e.g., a specified type of picture identification card). Each courier or escort will be issued a "Courier Certificate" and will be provided a list of possible secure storage locations and points of contact and emergency phone numbers (for business and non-business hours). The Courier Certificate and security responsibility briefings from Multinational Industrial Security Working Group (MISWG) Document No. 1, "Arrangements for the International Hand Carriage of Classified Documents, Equipment and/or Components," both contained in the International Programs Security Requirements Handbook available on the Defense Security Service and Defense Institute of Security Assistance Management websites, should be used and included as an enclosure to the Transportation Plan. For recurring shipments, this section will describe the standard requirements for use of the courier or escort and the details for each shipment, including the identity of couriers or escorts, will appear in the "Notice of Classified Consignment".]

H. RECIPIENT RESPONSIBILITIES. [Describe the specific responsibilities of the recipient Government for making arrangements with its port security and Customs officials to facilitate entry of the shipment into the recipient country, including the identification of points of contact and alternates at the debarkation location. Indicate where the Government-to-Government transfer will be completed. If the location is other than the port of debarkation, explain how the consignment will be moved to the specified location and the responsibility and procedures for such movement. Also describe the responsibility of the recipient Government's DGR to inventory the material and receipt for the consignment and its contents at the specified location, including specifically how:

1. The recipient organization will notify its Government security authority and the DGR of the dispatching organization of any deviation in the routes or methods prescribed in the Transportation Plan.

2. The recipient organization will notify its security authority and the DGR of the dispatching organization of any discrepancies in the documentation, damage or tampering with the packaging, or shortages in the consignment.

3. The recipient organization or Government will advise the DGR of the dispatching organization of any known or suspected compromise of classified material or any other exigencies that may have placed the consignment in jeopardy.

4. The recipient DGR will sign for the contents of the package and return a copy of the receipt to the dispatching organization.]

Figure C3.F5. Sample Transportation Plan for the Transfer of Classified Material (cont)

I. TRANSFER DOCUMENTATION: [Identify the documentation that is related to the shipment, including packing list, receipts, inventories, letter of offer and acceptance, export license, bill of lading, air waybill, signature and tally record, and declarations that my be required by law or regulation, etc.]

J. RETURN OF MATERIAL. [This section will identify any requirements for the return of classified material to the manufacturer or Government entity in the dispatching country (e.g., for warranty, repair, test, calibration etc.). The information provided will of necessity be general in nature. However, the basic requirement for a return Transportation Plan and methods to be used will be documented in the original Transportation Plan. The specific information required for an individual return shipment subsequently may be described in a Notice of Classified Consignment.]

Annex

NOTICE OF CLASSIFIED CONSIGNMENT TO TRANSPORTATION PLAN FOR

[Insert name and military nomenclature of the defense article or technical data]

AUTHORIZATION: [Insert the FMS Case Designator, License Number, Authorization Letter, or ITAR Exemption.]

1. PURPOSE. This annex describes procedures for the transfer by commercial carrier of the below listed items sold pursuant to [cite the FMS Case Designator, Export License, Authorization Letter, or Exemption]. If an ITAR Exemption is cited, identify the underlying authorization; e.g., FMS Case, License, etc. between [insert the name and address of the U. S. military depot or contractor facility] and [insert the name and address of the Government organization, contractor facility, or international organization] in [insert the identity the country].

2. DESCRIPTION OF CONSIGNMENT. [Insert a specific, detailed description of the end-items, parts, assemblies, sub-assemblies, software, test equipment, components, technical documents, etc. to be transferred under the annex, including the military nomenclature when applicable, and serial numbers; the number of packages or containers; a description of the packages or containers (e.g., the material of which they are constructed and the size and weight); and the numerical count of each item to be transferred in each package or container.]

3. IDENTIFICATION OF RESPONSIBLE GOVERNMENT AND/OR COMPANY OFFICIALS. [If the information was covered in the basic Transportation Plan, and has not changed, refer to the applicable section of the basic Transportation Plan. If the identity or other information related to any the persons in the basic Transportation Plan has changed, or the information was not covered in the basic Transportation Plan, include in this paragraph all of the information specified for section C of the Transportation Plan.]

4. IDENTIFICATION COMMERCIAL ENTITIES INVOLVED IN EACH TRANSFER. [If the information was covered in the basic Transportation Plan, and has not changed, refer to the basic Transportation Plan. If the identity or other information related to any the carriers, facilities or persons in the basic Transportation Plan has changed, or the information was not covered in the basic Transportation Plan, include in this paragraph all of the information specified for section D of the Transportation Plan.]

5. ROUTING OF CONSIGNMENT. [Unless the information is specifically covered in the basic approved Transportation Plan, the following information must be provided for each shipment. If the information is covered in the basic Transportation Plan, reference the applicable section of that Plan.]

Figure C3.F5. Sample Transportation Plan for the Transfer of Classified Material (cont)

a. Identity of Mode of Transport: [For each segment of the transfer (from point of origin to ultimate destination), identify the carriers to be used and include the name and address and the identity of a point of contact and an alternate (including telephone, cell phone, and telefax numbers, and e-mail addresses, both business and non-business hours) at all carriers. Include the flight, rail, or ship number, or other means of identifying the specific aircraft, vessel, or vehicle to be used, as well as the identity of the captain or other on-board representative who has been briefed on the arrangements for the shipment and is to provide assistance.]

b. Routes: [Describe the routes to be used between the point of origin of the shipment, the point of export from the country of origin, the point of import into the recipient country and the ultimate destination point (identify any specific programmed stops, layovers or transfer points; use codes that appear in Transportation Plan, if applicable).]

c. Dates and Times of Departure: [Provide the established date and time for each segment of the transfer.]

d. Date and Estimated Time of Arrival: [Provide the estimated date and time of arrival of the final carrier at the port in the country of destination.

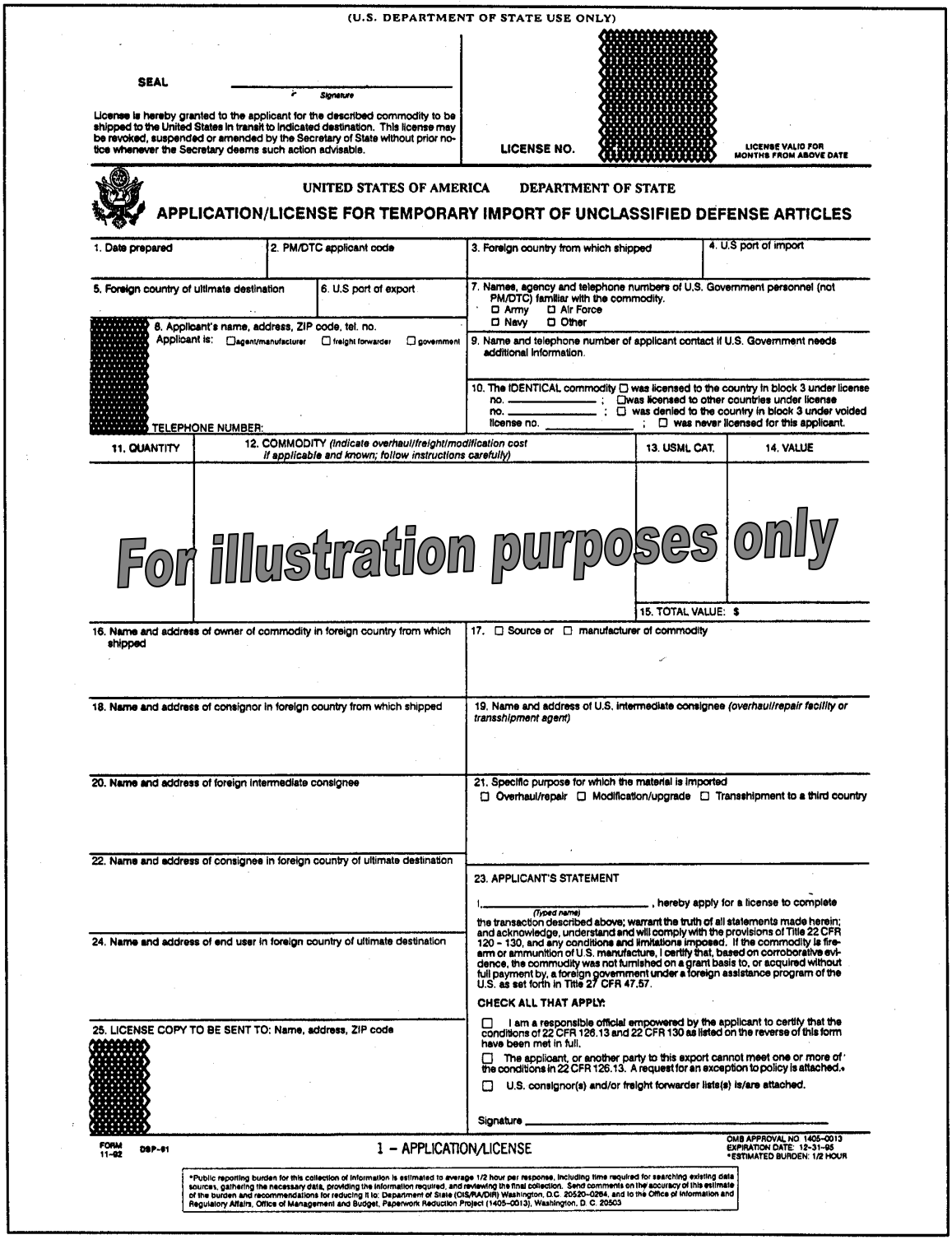
e. Freight Forwarders/Transfer Agents/Customs Brokers: [Identify the companies and their names and addresses, and the identity of a point of contact and an alternate (including the telephone, cell phone, and telefax number and e-mail address, both business and non-business hours) at the companies to be used, if they are not specified in the approved basic Transportation Plan. If the information is in the approved Plan, reference the applicable section. The security officer or DGR at the releasing depot or facility must verify the clearance and safeguarding capability of these entities, prior to the release of the consignment.]

f. Customs and Port Security Contacts: [Provide the name of a point of contact and an alternate at all ports, together with their telephone, cell phone, and telefax numbers and email addresses (for business and non-business hours), if they are not listed in the approved Transportation Plan. If they are so listed, reference the applicable section of the Plan.]

g. Emergency Procedures: [Provide the procedures to be followed for each segment of the transfer, and the names of points of contact and alternates in each country who are to be contacted in the case of an emergency. Provide telephone, cell phone, and telefax numbers and email addresses (for business and non-business hours).]

6. NAME(S) AND IDENTIFICATION OF COURIER/ESCORT. [Provide their full names, passport numbers and secondary identification, courier orders number and issuing authority, and the name and telephone and telefax number and e-mail address of an official that Customs or security authorities may contact, if further identification is necessary.]

Figure C3.F6. Department of State Form, DSP-61, Application/License for Temporary Import of Unclassified Defense Articles



(U.S. DEPARTMENT OF STATE USE ONLY)

SEAL _____ Signature

License is hereby granted to the applicant for the described commodity to be shipped to the United States in transit to indicated destination. This license may be revoked, suspended or amended by the Secretary of State without prior notice whenever the Secretary deems such action advisable.

LICENSE NO. [redacted] LICENSE VALID FOR MONTHS FROM ABOVE DATE

UNITED STATES OF AMERICA DEPARTMENT OF STATE

APPLICATION/LICENSE FOR TEMPORARY IMPORT OF UNCLASSIFIED DEFENSE ARTICLES

1. Date prepared	2. PM/DTC applicant code	3. Foreign country from which shipped	4. U.S port of import
5. Foreign country of ultimate destination	6. U.S port of export	7. Names, agency and telephone numbers of U.S. Government personnel (not PM/DTC) familiar with the commodity. ☐ Army ☐ Air Force ☐ Navy ☐ Other	
8. Applicant's name, address, ZIP code, tel. no. Applicant is: ☐agent/manufacturer ☐ freight forwarder ☐ government TELEPHONE NUMBER:		9. Name and telephone number of applicant contact if U.S. Government needs additional information.	
		10. The IDENTICAL commodity ☐ was licensed to the country in block 3 under license no. _____ ; ☐was licensed to other countries under license no. _____ ; ☐ was denied to the country in block 3 under voided license no. _____ ; ☐ was never licensed for this applicant.	

11. QUANTITY	12. COMMODITY *(Indicate overhaul/freight/modification cost if applicable and known; follow instructions carefully)*	13. USML CAT.	14. VALUE
			15. TOTAL VALUE: $

For illustration purposes only

16. Name and address of owner of commodity in foreign country from which shipped	17. ☐ Source or ☐ manufacturer of commodity
18. Name and address of consignor in foreign country from which shipped	19. Name and address of U.S. intermediate consignee *(overhaul/repair facility or transshipment agent)*
20. Name and address of foreign intermediate consignee	21. Specific purpose for which the material is imported ☐ Overhaul/repair ☐ Modification/upgrade ☐ Transshipment to a third country
22. Name and address of consignee in foreign country of ultimate destination	23. APPLICANT'S STATEMENT
24. Name and address of end user in foreign country of ultimate destination	I, _____ *(Typed name)*, hereby apply for a license to complete the transaction described above; warrant the truth of all statements made herein; and acknowledge, understand and will comply with the provisions of Title 22 CFR 120 – 130, and any conditions and limitations imposed. If the commodity is firearm or ammunition of U.S. manufacture, I certify that, based on corroborative evidence, the commodity was not furnished on a grant basis to, or acquired without full payment by, a foreign government under a foreign assistance program of the U.S. as set forth in Title 27 CFR 47.57.
25. LICENSE COPY TO BE SENT TO: Name, address, ZIP code [redacted]	CHECK ALL THAT APPLY: ☐ I am a responsible official empowered by the applicant to certify that the conditions of 22 CFR 126.13 and 22 CFR 130 as listed on the reverse of this form have been met in full. ☐ The applicant, or another party to this export cannot meet one or more of the conditions in 22 CFR 126.13. A request for an exception to policy is attached.* ☐ U.S. consignor(s) and/or freight forwarder lists(s) is/are attached. Signature _____

FORM DSP-61 11-02 1 – APPLICATION/LICENSE OMB APPROVAL NO. 1405-0013 EXPIRATION DATE: 12-31-95 *ESTIMATED BURDEN: 1/2 HOUR

*Public reporting burden for this collection of information is estimated to average 1/2 hour per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (CIS/RA/DIR) Washington, D.C. 20520-0284, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Paperwork Reduction Project (1405-0013), Washington, D. C. 20503