CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J6 CJCSI 6510.06B
DISTRIBUTION: A, B, C, S 31 March 2011

COMMUNICATION SECURITY RELEASES TO FOREIGN NATIONS

References: See Enclosure D.

1. Purpose. This instruction establishes policy and procedures for:

a. Disclosing, releasing, and transferring information systems security (INFOSEC) products or associated communications security (COMSEC) information to foreign governments in accordance with DODI 8523.01, "Communications Security (COMSEC)" (reference a). Disclosures, releases, or transfers to international organizations (e.g., NATO) are not under the cognizance of the Chairman of the Joint Chiefs of Staff and are not addressed in this instruction (see National Security Telecommunications and Information Systems Security Policy No. 8, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated COMSEC Information to Foreign Governments" (reference b)).

b. COMSEC products or associated COMSEC information support to foreign nations under ship rider procedures.

c. Negotiating and concluding international COMSEC agreements.

d. Establishing the Command and Control Interoperability Board (CCIB) as it relates to communications interoperability and security memorandums of agreements (CIS MOAs) covered in this instruction.

e. Developing COMSEC Release Request (CRR) messages and their required communication and coordination paths towards validation and approval.

f. Releasing Department of Defense procedural message standards required by CIS MOAs.

2. Cancellation. CJCSI 6510.06A dated 18 December 2006 is canceled.

3. Applicability. This instruction applies to the Chairman of the Joint Chiefs of Staff (CJCS), the Joint Staff, the combatant commands, the Military Departments, their respective Services, the Defense Agencies, Weapon System Program Management Offices (PMOs,) and DOD field activities (hereafter referred to as DOD components) that require the release of COMSEC or associated COMSEC information to foreign governments. It further applies to the U.S. Coast Guard when undertaking DOD missions. Nothing in this instruction alters or supersedes the existing authorities of the Director of National Intelligence (see Committee on National Security Systems Directive No. 502, "National Directive on Security of National Security Systems [reference c]). Secure communications requirements with foreign national entities not addressed by this instruction should be referred to the Joint Staff and National Security Agency (NSA) for further guidance.

4. Policy. See Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes. This revision incorporates changes to promote greater communication and coordination between the combatant commands, the Services, PMOs, the Joint Staff, and NSA to better define interoperability needs with our growing array of coalition partners. Significant changes include:

a. Clarifies guidance for COMSEC Release Requests (CRRs) for non-NATO nations in support of NATO and NATO nations in support of bilateral combatant command requirements.

b. Adds guidance to address procedures for short notice/urgent CRRs.

c. Clarifies guidance on the CRR process with updates to the COMSEC release procedure language and associated flow chart.

d. Updates CRR boilerplate to reflect the need for greater detail in defining the secure interoperability requirement and in providing detailed technical descriptions of the interoperability requirement and environment.

e. Adds combatant command and Joint Staff requirements to address additional concerns for CRRs including COMSEC devices that provide or are related to intelligence, surveillance, and reconnaissance (ISR) capabilities.

8. Releasability. This instruction is approved for limited release. DOD components (to include the combatant commands) and other federal agencies may obtain copies of this instruction through controlled Internet access only (limited to .mil and .gov users) from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives. Joint Staff activities may access or obtain copies of this instruction from the Joint Staff Resources Portal--http://jointstaff.js.smil.mil/portal/site/jsportal/jelinstructions.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

WILLIAM E. GORTNEY
Vice Admiral, USN
Director, Joint Staff

Enclosure(s):

A – Policy
B – Responsibilities
C – Procedures for COMSEC Release Request (CRR)
D – References
Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, and C plus the following:

	Copies
Secretary of State	2
Secretary of Defense	2
Secretary of Homeland Security	2
Director of National Intelligence	2
Director of Central Intelligence	2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

FIGURE PAGE

ENCLOSURE A

POLICY

1. Criteria for Release of COMSEC Products and Information. The Chairman of the Joint Chiefs of Staff (hereinafter "Chairman") will validate combatant command interoperability requirements to release COMSEC products or associated COMSEC information to any foreign government (including Combined Communications-Electronics Board (CCEB),[i] NATO nations, and non-NATO nations). COMSEC interoperability requirements originating from the Military Departments, their respective Services, the Defense agencies, PMOs, and the DOD Field Activities must be reviewed by all affected combatant commands in which the foreign partner resides and operates. When a request crosses multiple command areas of responsibility (AORs), only a single combined request is required (see Cross-Combatant Command section in Enclosure A, paragraph 8). These requests also require Joint Staff review and validation. Combatant commands may recommend the desired solution; however, the Director of the National Security Agency (DIRNSA) will select the appropriate COMSEC solution, and the Committee on National Security Systems (CNSS) will determine releases in accordance with NSTISSP 8 (reference b). In all cases, the most important criteria supporting a COMSEC release are the combatant command validation and/or endorsement of an emerging or documented interoperability requirement requiring secure communications. An ally or coalition partner's desire to be interoperable with a U.S. combatant command is not, in and of itself, sufficient justification for such releases.

a. All requests for release of U.S. government (USG) COMSEC products or associated COMSEC information must:

(1) Be consistent with USG foreign policy and military or economic objectives;

(2) Have no unacceptable impact on USG signals intelligence (SIGINT) activities; and

(3) Not impact adversely on the overall INFOSEC posture of the USG.

b. In addition, requests must meet at least one of the two criteria detailed below:

(1) Enhance the objectives and effectiveness of mutual USG defense arrangements or coalition operations by providing a means for achieving secure communications interoperability when exchanging military planning

[i] CCEB Nations include the United States, Canada, United Kingdom, New Zealand, and Australia.

information or conducting combined or coalition combat operations that involve U.S. military forces and the military forces of a foreign government(s).

(2) Protect USG national security information that is provided to or exchanged with a foreign government in support of USG efforts to combat the transnational threats of international crime, international terrorism, international drug trafficking, or proliferation of weapons of mass destruction. The Joint Staff may request combatant command endorsement of requirements involving said transnational threats.

2. Limitations. Provided the criteria in paragraph 1 of this enclosure are satisfied, the following limitations apply to the release of COMSEC products or associated COMSEC information:

a. COMSEC products or associated COMSEC information included in weapons, communications, or other major defense systems to provide a complete package for Foreign Military Sales (FMS), or initiatives to promote international competition for system procurements, are not, in and of themselves, acceptable justifications for seeking release of those products or information.

b. U.S. COMSEC products or associated COMSEC information will not normally be authorized for release solely for purposes of improving the internal national INFOSEC posture of a foreign government.

3. Discussions With Foreign Nations

a. Policy of False Impression. Refer to National Disclosure Policy 1 (NDP-1), "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations" (reference d), for all issues regarding establishment of a false impression regarding U.S. commitment to release of classified material. The national disclosure authority of COMSEC products or associated COMSEC information is the CNSS.

b. Authorization for Discussions. An approved release in principle (RIP) or release in specific (RIS) is required before initiating discussions on disclosure or release of U.S. COMSEC information to a foreign government by any DOD component.

(1) Before initiating discussions or negotiations on weapon systems; command, control, communications, computers and intelligence (C4I) systems; or other U.S. platform COMSEC products and associated COMSEC information, DOD components must define the need, or expected need through a CRR that clearly identifies the interoperability requirement with the foreign partner.

(2) When the use of COMSEC products or associated COMSEC information is implied or possible but not absolutely required, discussions may be conducted. However, no COMSEC products or associated COMSEC information may be committed or discussed other than to acknowledge that some type of USG or authorized/approved commercial COMSEC products may be required.

4. Exception to the National Disclosure Policy (ENDP). An ENDP may be required to approve the release of USG information that will be protected by COMSEC products released under this instruction. The Joint Staff, Military Services, and Defense agencies initiate ENDP requests in accordance with NDP-1 (reference d) and DODD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations" (reference e), to approve the type and level of classification of information to be exchanged with foreign nations. Combatant commands' ENDP requests shall be submitted via memorandum to Joint Staff J-5 for forwarding to the National Disclosure Policy Committee.

5. Committee on National Security Systems. The CNSS is the USG authority on the **release** of COMSEC products or associated COMSEC information to foreign governments. CNSS does not, however, review or approve DOD bilateral COMSEC agreements, Communications Interoperability and Security Memorandums of Agreement (CIS MOAs), and INFOSEC equipment agreements (IEAs), which are governed by DODD 5530.3, "International Agreements" (reference f). Refer to NSTISSP-8 (reference b) for CNSS/DIRNSA responsibilities, urgent requirements, membership, and other issues related to the CNSS. Additional information regarding the CNSS can be found at www.cnss.gov.

6. NATO Nations. Release of COMSEC products or associated COMSEC information to NATO or NATO member nations also requires approval by the CNSS or national manager as outlined in reference b.

a. COMSEC releases to support NATO interoperability (i.e., communications between and among components of the NATO military, political, and civil infrastructure and between that infrastructure and the NATO nations when conducting NATO activities, and common defense responsibilities under the North Atlantic Treaty) are not governed by this instruction and do not require validation from the Joint Staff. Appropriate NATO agreements, policy, and procedures describe the infrastructure by which the United States can provide U.S. COMSEC products and information to NATO nations and the NATO infrastructure to satisfy NATO secure interoperability requirements. (See SDIP-293, "Instructions for the Control and Safeguarding of NATO Cryptomaterial" (reference g); AC/35-D, "NATO Security Committee Primary Directive on INFOSEC" (reference h); MC 74/3

Corrigendum 3, "Communications Security for NATO" (reference i); and Document C-M(2002)49, "Security Within the North Atlantic Treaty Organization" (reference j).) These documents also preclude the need for a separate CIS MOA or IEA with NATO or with NATO nations. COMSEC release requests to support NATO interoperability requirements shall be forwarded by the United States Military Delegation to NATO (USDELMC) to the NSA DP-2 NATO desk for processing. For the purpose of combatant command endorsement and situational awareness, the USDELMC should inform all affected combatant commands of the COMSEC products being utilized by NATO nations residing or operating in the combatant command's AOR.

b. COMSEC release requests to support NATO interoperability requirements with non-NATO countries (i.e., Partners for Peace countries, Mediterranean Dialog nations, Istanbul Cooperation Initiative nations, and other non-NATO nations) will be forwarded by the USDELMC to the appropriate geographic combatant command. The combatant command will assess its ability to support (endorse) the NATO interoperability requirement and submit a CRR in accordance with paragraph 7, below. If the non-NATO country resides in a different geographic combatant command AOR, the interoperability requirement should be submitted as a cross-combatant command CRR in accordance with paragraph 8, below.

c. When a COMSEC release request is for the sole purpose of supporting bilateral interoperability requirements between a NATO nation and a combatant command and there is no NATO interoperability requirement, the combatant command must submit a standard CRR or cross-combatant command CRR as applicable.

7. Types of COMSEC Releases. There are two types of release approvals for COMSEC products and associated COMSEC information.

a. Release in Principle. A RIP provides a USG policy decision related to disclosure of COMSEC information, products, or services in support of a secure interoperability requirement. **A RIP is not an approval to physically transfer any COMSEC products.** A RIP is required prior to combatant commands, U.S. Military Services and their components, and DOD departments and agencies having detailed discussions with the foreign nation regarding COMSEC products or associated COMSEC information requirements and in developing proposed solutions to fulfill U.S. secure interoperability requirements. A RIP is not required if either the technical requirements that the COMSEC products/information must support can be identified or the quantity of products/information can be specified without having a detailed discussion with the foreign nation. In such cases, a RIS should be used.

b. Release in Specific. A RIS provides USG approval for release of a defined set (quantity and nomenclature) of COMSEC information, products, or services

to a foreign partner. Using the procedures in Enclosure C of this document, the combatant command submits a CRR that defines an interoperability requirement and recommends a number of devices. If the requirement is validated by the Joint Staff, then the DIRNSA, serving as national manager, as designated in NSD-42, "National Policy for the Security of National Security Telecommunications and Information Systems" (reference k), will identify and recommend to the CNSS the appropriate COMSEC solution and quantity of devices to release.

(1) For previously Joint Staff validated interoperability requirements that are not significantly modified from the terms of the original release (e.g., location, network, quantity, or type of COMSEC device required), the requesting command or agency may submit the CRR directly to the DIRNSA. In those instances where minor changes have been made, the combatant command or agency must first seek approval from the Joint Staff before going directly to the DIRNSA with an amended requirement. If the interoperability requirement has changed, a new CRR shall be submitted to the Joint Staff for validation.

(2) Based on the technical details of the fundamental communications/ interoperability requirement, a RIS must identify the type of equipment, quantity, location/destination, intended purpose, etc., to be released. If a detailed discussion with a foreign nation is required to identify those fundamental requirements, a RIP, rather than a RIS, should be used.

(3) General Releases. A general release is a RIS approval that does not limit the quantity of COMSEC devices or tie the approval to a specific weapon system or platform. Once a general release is approved, the foreign nation may purchase products as needed through FMS or Direct Commercial Sales (DCS) channels as authorized by the DIRNSA. Due to the special nature of some countries and the need for greater control of releasing these devices to those countries, a combatant command may elect to NOT request a general release for the below devices. They may instead request a RIS for each specific requirement. General releases apply only to the following COMSEC products and services:

(a) Global Positioning System (GPS) -- Precise Positioning Service (PPS). Includes legacy and Selective Availability Anti-Spoofing Module (SAASM) based PPS Host Application Environment (HAE).

(b) MODE 4 identification friend or foe (IFF).

8. Cross-Combatant Command Requirements. A cross-combatant command requirement is one in which military forces from a foreign partner in one combatant command's AOR are operating in direct support of coalition initiatives in another combatant command's AOR. For example, a country from

the U.S. Pacific Command AOR is supporting coalition operations in the U.S. Central Command (USCENTCOM) AOR. USCENTCOM as the supported combatant command (i.e., "gaining" combatant command) assumes all responsibility for ensuring secure interoperability with the foreign nation. This includes "reachback" requirements for coalition partners. The supported combatant command is required to submit all CRRs in coordination with the foreign partner's natural combatant command. This coordination will help maintain U.S. military situational awareness of the partner's secure communications capabilities for future joint operations.

Note: If the released COMSEC devices are on a short-term loan, then the supported combatant command is responsible for ensuring the return of all released COMSEC at the conclusion of the requirement.

9. Short-Notice/Urgent and Crisis Action Procedures. In the event that a CRR requires expedited processing to meet emerging/immediate operational requirements, the combatant command shall inform the Joint Staff action officer and the NSA desk officer of the requested expedited timeline at CRR submission. The below procedures apply to operational requirements only. Expedited processing will not be accepted in order to meet FMS or exercise COMSEC release requirements.

a. The Joint Staff will provide instructions for chain of command notification (i.e., phone call or e-mail from senior member in combatant command chain of command to justify the expedited requirement) based on the urgency of the request. Short-notice requests will receive accelerated validation processing, while urgent requests will receive immediate validation processing.

b. When a request meets the criteria for crisis action procedures, i.e., there are urgent requirements where U.S. lives may be at risk and time and circumstances preclude a formal CRR submission, the combatant command shall request Joint Staff validation and COMSEC release approval from the DIRNSA via any communications path necessary. If necessary, the DIRNSA will seek expedited release approval from the CNSS in accordance with NSTISSP-8 (reference b). For recordkeeping purposes, crisis action procedures still require combatant commands to submit a formal CRR and complete the entire RIS process as soon as possible after the expedited transfer takes place.

10. Bilateral Agreements. Combatant commands shall execute bilateral agreements with non-CCEB and non-NATO nations prior to physically transferring COMSEC products and services. The agreement shall outline each party's responsibilities and identify the minimum safeguards required to protect COMSEC material.

a. Communications Interoperability and Security Memorandum of Agreement. Any transaction involving the FMS or Foreign Military Sales-Cryptographic Device Services (FMS-CDS) transfer of U.S. COMSEC products or information to a non-NATO, non-CCEB foreign nation requires a CIS MOA. CIS MOAs provide the legal framework and mechanism for the long-term transfer (sale, loan, or FMS-CDS transfer) and safeguarding of COMSEC products and information and configuration management (CM) specifications necessary to establish and enhance long-term strategic partnerships and mutual Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) endeavors.

(1) Accountability of COMSEC products and information transferred under a CIS MOA is provided through the establishment of a dedicated, U.S.-staffed COMSEC account as outlined in Appendix B to Enclosure C, or through the use of a formally established COMSEC account recognized by the United States. The CIS MOA further provides for the establishment of a Command and Control Interoperability Board (CCIB), a bilateral and multidisciplinary forum for addressing combined interoperability initiatives on a mutually agreeable basis. CIS MOAs are valid for a maximum of 15 years.

(2) In accordance with DODD 5530.3 (reference f), CJCSI 2300.01D, "International Agreements" (reference l), and CJCSI 6740.01B, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations" (reference m), the DIRNSA provides the authority to negotiate and conclude the COMSEC portion of a CIS MOA, and the Joint Staff provides authority to negotiate and conclude the CM portion. The Joint Staff formally notifies the combatant command that the DIRNSA and Joint Staff have delegated authority to negotiate and conclude a CIS MOA to the combatant command.

b. INFOSEC Equipment Agreement (IEA). IEAs provide the legal framework between the DOD and any foreign military partner for the short-term and/or isolated loan and safeguard of COMSEC products and information. "Loan," in this context, refers to a combatant command or other USG agent temporarily allowing a foreign nation to use releasable COMSEC products or information purchased by the U.S. sponsor. The term does not imply any form of sale, FMS-CDS transaction, or any long-term transfer. An IEA should not be used if the duration of the loan is expected to be the same as the effective life of the loaned equipment . Accountability of COMSEC products and information transferred under an IEA is the responsibility of the issuing combatant command, component command, or other USG departments or agencies. Accountability will be maintained within existing COMSEC material control system (CMCS) infrastructure of the issuing agency; however, the combatant command may also request support from its component commands or other USG departments or agencies. When component command COMSEC accounts are used to support an IEA, the combatant command will document and

provide all relevant information (e.g., name and security clearance) to the custodian to authorize release of the COMSEC equipment. Unlike a CIS MOA, an IEA does not provide for the establishment of a CCIB. The DIRNSA provides the authority for a combatant command to negotiate and conclude an IEA. Signed IEAs must be on file with NSA before any COMSEC products or information are transferred.

c. A COMSEC Material Report Form (SF-153). An SF-153 will be used to temporarily transfer COMSEC equipment to a foreign nation to support operational/exercise requirements in which time does not permit negotiation of either of the above agreements. The SF-153 must include the following paragraph:

"This equipment is hereby loaned for secure data/voice interoperability with U.S. and Coalition forces. I, the undersigned, certify that I am aware of and will provide the safeguards required for this material. I will implement the minimum security safeguards as dictated in the attached operational COMSEC doctrine. Equipment listed on this form will remain the property of the U.S. government; I do not have authority to sell, dispose of, or transfer the equipment; this equipment will not be reverse engineered in any fashion; and will be made available whenever required during periodic COMSEC inventories for viewing and inspection by authorized U.S. COMSEC personnel. This equipment must be returned to the U.S. government upon request or completion of the secure interoperability requirement. I understand that I will be required to sign an updated receipt when additional material is made available."

d. Combatant commands shall initiate the negotiation process of a CIS MOA or IEA by submitting a request for delegation of authority to negotiate and conclude within 90 days of any release approval signed by the CNSS in anticipation of a signed agreement. The transfer of COMSEC devices will not occur until the appropriate bilateral agreement is adjudicated and agreed to by both parties. Failure of a foreign partner to initiate the appropriate agreement after 90 days of a signed release will result in revocation of the release approval. It is incumbent upon the combatant commands to hold or reacquire the released devices from any foreign partner refusing to sign previously agreed upon bilateral agreements (or updates) that legally protect U.S. COMSEC in their possession. Exceptions can be made for those partners working in good faith to secure signatures but are having scheduling difficulties.

11. COMSEC Transfer Mechanisms. National policy governing the transfer of all defense articles and services is outlined in Executive Order 11958, "Administration of Arms Export Controls" (reference n). National policy specifically governing the transfer of U.S. COMSEC products and information is outlined in NACSI 6001, "Foreign Military Sale of Communications Security Articles and Services to Foreign Governments and International Organizations"

(reference o). All transfers of U.S. COMSEC products and information, including all COMSEC and cryptographic systems, whether standalone or embedded in other platforms, are under the cognizance of the DIRNSA. The CJCS delegation of acquisition authority, development authority, or distribution authority over platforms that have inherent COMSEC equipment (e.g., aircraft, ships, tanks) does not imply delegation of authority to release the inherent COMSEC equipment to foreign nations.

a. Direct Commercial Sale. DCS involves the direct purchase by foreign governments of COMSEC products from authorized U.S. commercial vendors. The DIRNSA has authorized DCS for COMSEC products under the following guidelines:

(1) DCS to CCEB Nations. CCEB nations may purchase select COMSEC products through DCS channels. The DIRNSA must specifically authorize the U.S. vendor to sell a particular COMSEC product via DCS.

(2) GPS-PPS/SAASM and MODE 4 IFF COMSEC products. Nations for which the CNSS has approved the release of GPS-PPS/SAASM and MODE 4 IFF COMSEC products may purchase those products via DCS if specifically authorized by the DIRNSA on a case by case basis. The DOD GPS Security Policy (reference p) provides further guidance on the sale of GPS-PPS/SAASM.

b. Foreign Military Sales (FMS). FMS involves the sale of defense articles/services to foreign governments. The DIRNSA has authorized FMS for COMSEC products under the following guidelines:

(1) FMS to CCEB and NATO Nations. FMS is the primary mechanism for the sale of COMSEC products approved for release to CCEB and NATO Nations. FMS cases for COMSEC devices may be managed by the DIRNSA or the DIRNSA may delegate that authority for specific cases and/or devices to other DOD implementing agencies.

(2) GPS-PPS/SAASM and MODE 4 IFF COMSEC products. Nations for which the CNSS has approved the release of GPS-PPS/SAASM and MODE 4 IFF COMSEC products may purchase those products via FMS. The DIRNSA has delegated to other DOD implementing agencies authority to manage FMS cases for GPS-PPS/SAASM and MODE 4 IFF COMSEC products. (This section applies to all nations.)

c. Foreign Military Sales -- Cryptographic Device Services. This section applies to non-CCEB and non-NATO Nations. FMS-CDS consists of the sale of COMSEC services (the use of a COMSEC product) rather than the actual sale of the product itself. In all FMS-CDS cases, the United States retains legal title to the COMSEC product and can recall the COMSEC product at any time. Every effort will be made by combatant command interoperability planners to

avoid reclaiming devices at the expense of the partner if due to no fault of their own. If, however, the items are recalled for violations of signed agreements, the foreign partner is required to return the devices immediately to the USG without reimbursement. These title and recall stipulations to FMS-CDS sales are clearly identified in the associated FMS case. FMS-CDS is used to transfer special purpose (S-type) and other COMSEC products to non-CCEB and non-NATO nations in support of Joint Staff validated interoperability requirements. S-type COMSEC products are provided only to non-CCEB and non-NATO nations and are interoperable with the respective K-Type COMSEC products. All FMS-CDS cases must be directly associated with an approved RIS in support of Joint Staff validated interoperability requirements. FMS-CDS cases for S-type COMSEC products are always handled by NSA. Management of FMS-CDS cases for non-S-type COMSEC products may be delegated to other DOD implementing agencies. All sales or loans of ancillary products associated with COMSEC products (e.g., key fill products, cables, and racks) to coalition nations will be managed by NSA through FMS-CDS cases or delegated to other DOD implementing agencies.

d. COMSEC Equipment Loans. A loan involves the purchase of COMSEC products by a DOD organization and the temporary transfer to a foreign partner for a short duration of time. The foreign nation does not at any time own the equipment. COMSEC equipment loans are valid for a limited time period and are subject to the terms of the bilateral agreement governing the loan, and to Section 421 of Title 10, U.S. Code, "Armed Forces" (reference q).

12. Next-Generation COMSEC Products

a. Next-Generation COMSEC products are devices designed as follow-on replacements for existing COMSEC solutions or those that provide a new COMSEC capability. Release of current-generation equipment does not necessarily imply release of next-generation equipment. Combatant commands shall submit new CRRs for next-generation COMSEC products to the Joint Staff for validation of new requirements and submit CRRs for existing requirements to the DIRNSA.

b. The DIRNSA will establish policy guidelines, in coordination with the Joint Staff and combatant commands, which outline next generation cryptographic modernization efforts specifically addressing implementation plans for critical next generation efforts such as Mode 5 and Software Defined Radio (SDR) platforms so that U.S. interoperability is ensured with coalition partners.

c. If a combatant command, Service, or Defense agency wishes to interoperate with a country using Suite B products, it will still be required to submit a CRR to the Joint Staff and the NSA if any U.S.-generated key materials, U.S. key loaders, or other supplemental U.S. COMSEC hardware

must be transferred to the country in order to complete the proposed secure communications solution. If, however, Suite B products are used without requiring the transfer of the above items to the foreign partner, a CRR is not required.

13. Ship Rider Procedures

a. A ship rider is a DIRNSA-authorized procedure allowing properly cleared U.S. personnel to temporarily install, operate, key, and physically secure and provide 24-hour control for U.S. COMSEC products or associated COMSEC information in foreign nation sites or platforms.

b. Ship rider procedures are not releases of COMSEC products or associated COMSEC information to foreign countries. These procedures may be used to solve unique, short-term interoperability requirements for combined operations or training exercises.

c. Under ship rider procedures, the DIRNSA recommends a minimum of three U.S. personnel to provide this service under normal circumstances. Certified U.S. personnel will remove all COMSEC products and information from foreign-controlled spaces as soon as possible after the exercise or operation ends.

d. Under ship rider procedures, foreign nationals are not permitted unaccompanied access to any U.S. COMSEC products or associated COMSEC information. Foreign nationals may not, at any time, have access to keying material for the products. Foreign nationals may be present when controlled cryptographic item (CCI) products are keyed by cleared U.S. personnel, but they are not permitted to load, handle, or have access to any keying material associated with the products.

e. A ship rider authorization does not relieve disclosure requirements as identified by NDP-1 (reference d).

f. Ship Rider Request (SRR) Authorization Request Format.

(1) The combatant command or Service sponsoring the exercise will submit an SRR via message or cryptographically signed e-mail (as it becomes available on the SIPRNET) to the DIRNSA (DIRNSA FT GEORGE G MEADE MD//DP2//). Note: The parties involved (NSA/DP2, Joint Staff, combatant commands, Services, and Defense agencies) will ensure e-mail connectivity by regularly updating point of contact (POC) addresses with counterpart offices. E-mail addresses change too frequently and thus will not be listed in this instruction.

(2) The following INFO addressees will be included on all SRR messages:

JOINT STAFF WASHINGTON DC//
SECDEF WASHINGTON DC//USDP:DSCA/USDP:ISA//
CNO WASHINGTION DC// N2N6F1 //
NAVY IPO WASHINGTON DC//02//
DA WASHINGTON DC//DUSA-IA//
OSAF WASHINGTON DC//IA//
USASAC ALEXANDRIA VA//AMSAC//

(3) The words “SHIP RIDER REQUEST (SRR)” will be included in the SUBJECT line.

(4) Section one should identify the interoperability requirement, the foreign nations involved, and the sponsor and name of the ongoing combined operation or combined training exercise.

(5) Section two should state the timeframe (start and stop) for the ship rider procedures.

(6) Section three should identify the foreign platforms or locations (i.e., ships, planes, vehicles, or headquarters) that will host the COMSEC products.

(7) Section four should identify the specific COMSEC nomenclature, products, and quantities.

(8) Sections five and six must include the following paragraphs, exactly as written below. Insert the appropriate foreign government and platform(s) in section 5.

> COMSEC PRODUCTS WILL BE TEMPORARILY INSTALLED ON [COUNTRY] [LOCATION/PLATFORM (EX. SHIP NAME)] ONLY BY U.S. GOVERNMENT PERSONNEL WITH THE APPROPRIATE SECURITY CLEARANCE AND ONLY FOR [DATES]. PROPERLY CLEARED U.S. PERSONNEL WILL OPERATE AND MAINTAIN THE PRODUCTS/ EQUIPMENT AND PROVIDE 24-HOUR CONTROL OF THE COMSEC PRODUCTS, EQUIPMENT, ASSOCIATED KEYMAT, AND KEY FILL AND KEY TRANSFER PRODUCTS. THESE PERSONNEL TEAMS WILL REMOVE THE COMSEC PRODUCTS AS SOON AS POSSIBLE AT THE CONCLUSION OF THE REQUIREMENT.
>
> THE SHIP-RIDER APPROVAL DOES NOT RELIEVE RESPONSIBILITY FOR MEETING NATIONAL DISCLOSURE POLICY (NDP) REQUIREMENTS FOR THE DISCLOSURE OF

CLASSIFIED MILITARY INFORMATION TO FOREIGN GOVERNMENTS.

g. The appendix to this enclosure is an example of the ship rider request.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE A

SHIP RIDER REQUEST EXAMPLE

DTG
FM COCOM
TO DIRNSA FT MEADE//DP2//
INFO JOINT STAFF WASHINGTON DC//
SECDEF WASHINGTON DC//USDP:DSCA/USDP:ISA//
CNO WASHINGTON DC//N2N6F1//
NAVY IPO WASHINGTON DC//02//
DA WASHINGTON DC//DUSA-IA//
OSAF WASHINGTON DC//IA//
USASAC ALEXANDRIA VA//AMSAC//
[ADDITIONAL APPLICABLE OFFICES]
BT
CLASSIFICATION//2202//
MSGID/GENADMIN/[REQUESTING COMMAND]//
SUBJECT: SHIP-RIDER REQUEST FOR COMSEC EQUIPMENT INSTALLATION IN SUPPORT OF [EXERCISE/ACTIVITY]./(CLASSIFICATION)//
REF/A/DOC/JOINT STAFF/[DATE OF THIS ISSUANCE]/CJCSI 6510.06B//
AMPN/REF A IS THE CJCS INSTRUCTION THAT OUTLINES STEPS FOR REQUESTING APPROVAL TO USE SHIP RIDER PROCEDURES.//
RMKS/1. (CLASSIFICATION) REQUEST TO USE SHIP RIDER PROCEDURES TO INSTALL, OPERATE AND MAINTAIN [COMSEC EQUIPMENT AND QUANTITY] OR LIKE DEVICE(S), ABOARD [COUNTRY] [LOCATION/PLATFORM (EX. SHIP NAME)].
2. (CLASSIFICATION) THIS SHIP RIDER REQUEST IS FOR THE PERIOD OF [DATES], IN SUPPORT OF [EXERCISE/ACTIVITY].
3. (CLASSIFICATION) THE ABOVE COMSEC EQUIPMENT SHALL BE TEMPORARILY INSTALLED ABOARD [COUNTRY] [LOCATION/PLATFORM (EX. SHIP NAME)].
4. (CLASSIFICATION) TYPES AND QUANTITIES OF SPECIFIC COMSEC PRODUCTS/EQUIPMENT ARE DETAILED BELOW:
SYSTEM COMSEC PRODUCT QUANTITY
5. (CLASSIFICATION) COMSEC PRODUCTS WILL BE TEMPORARILY INSTALLED ON [COUNTRY] [LOCATION/PLATFORM (EX. SHIP NAME)] ONLY BY U.S. GOVERNMENT PERSONNEL WITH THE APPROPRIATE SECURITY CLEARANCE AND ONLY FOR [DATES]. PROPERLY CLEARED U.S. PERSONNEL WILL OPERATE AND MAINTAIN THE PRODUCTS/EQUIPMENT AND PROVIDE 24-HOUR CONTROL OF THE COMSEC PRODUCTS, EQUIPMENT, ASSOCIATED KEYMAT AND KEY FILL AND KEY TRANSFER PRODUCTS. THESE PERSONNEL TEAMS WILL REMOVE THE COMSEC PRODUCTS AS SOON AS POSSIBLE AT THE CONCLUSION OF THE REQUIREMENT.

6. (CLASSIFICATION) THE SHIP RIDER APPROVAL DOES NOT RELIEVE RESPONSIBILITY FOR MEETING NATIONAL DISCLOSURE POLICY (NDP) REQUIREMENTS FOR THE DISCLOSURE OF CLASSIFIED MILITARY INFORMATION TO FOREIGN GOVERNMENTS.//
BT

ENCLOSURE B

RESPONSIBILITIES

1. The Joint Staff will:

a. Review for validation/non-validation new or amended interoperability requirements submitted by combatant commands for the proposed release of COMSEC products or associated COMSEC information to foreign partners through coordination within the Joint Staff. The Joint Staff will forward validated requirements to the DIRNSA for review, solution identification, and DIRNSA/CNSS approval. Validation indicates concurrence with the type of bilateral agreement identified by the combatant command to support the requirement. Validation also indicates Joint Staff concurrence that the requirement represents a legitimate U.S. military need for secure interoperability.

b. In the event that Joint Staff does not validate a proposed interoperability requirement, the Joint Staff will notify the combatant command formally with a written justification. The combatant command may elect to alter the nature of the requirement, provide sufficient justification to support the original requirement, or withdraw the proposed interoperability requirement.

c. In the event that NSA notifies the Joint Staff that a COMSEC solution is not available to meet the validated interoperability requirement due to a technology gap or a specific security concern, the Joint Staff will forward a formal response to the requesting combatant command.

d. Review and approve, in coordination with DISA, the CM portion of a CIS MOA. Pending DIRNSA approval of the COMSEC products and services portion of the CIS MOA, delegate authority to negotiate and conclude to the requesting combatant command.

e. Validate the combatant command's requirement for a CIS MOA and, upon notification from the DIRNSA and DISA of approval of their respective portions, delegate to the combatant command the final authority to negotiate and conclude the agreement.

f. Foster and facilitate greater communication between the International Program Offices (IPOs), Services, and the combatant commands to develop interoperability plans, CRRs, and bilateral agreements within the frameworks outlined in this document.

g. Notify DOD components of bilateral and coalition cooperative development efforts that require CRRs, CIS MOAs, or IEAs submitted by a combatant command.

2. Combatant Commands will:

a. Integrate C4I strategic plans that identify current and anticipated allied and coalition interoperability requirements requiring COMSEC solutions into a combatant command's Theater Campaign Plan (TCP).

b. Validate and/or endorse new interoperability requirements and submit CRRs to the Joint Staff and the DIRNSA. The controlling authority, if different from the requesting combatant command, should receive a courtesy copy.

c. Withdraw or alter CRRs that have not been validated by the Joint Staff or for which NSA determines a COMSEC solution is not available or cannot be developed within a reasonable amount of time to meet the validated interoperability requirement.

d. Staff and consider for endorsement USG, DOD, or applicable international organization interoperability requirements or activities in their AOR where the release of USG COMSEC products or information to a foreign partner or international organization is required.

e. Submit bilateral agreements to the appropriate authority as outlined below:

(1) CIS MOAs to the Joint Staff and the DIRNSA for authority to negotiate and conclude as prescribed in Enclosure A, paragraph 10.a. Once signed, provide reproducible copies to the General Counsel of the Department of Defense, Joint Staff, the DIRNSA, DISA, and DSCA.

(2) IEAs to the DIRNSA for authority to negotiate and conclude as prescribed in Enclosure A, paragraph 10.b. Once signed, provide reproducible copies to the General Counsel of the Department of Defense, the Joint Staff, and the DIRNSA.

(3) Document authorized and transferred COMSEC release documentation in accordance with Enclosure C, Appendix B, paragraph 6.

f. Oversee the establishment of an authorized COMSEC accounting mechanism, in accordance with the appropriate bilateral agreement, to safeguard COMSEC product(s) released to foreign nations.

(1) Sponsor the establishment of an NSA-recognized COMSEC account to support the transfer of COMSEC products under a signed CIS MOA.

(2) Support the International Program Offices (IPOs) in the implementation and coordination efforts for ensuring COMSEC support to COMSEC custodians of NSA-recognized COMSEC accounts that support a signed CIS MOA.

(3) Perform periodic audits and semiannual inventories of the account, in coordination with and in support of NSA and in accordance with NSA/CSS Policy Manual 3-16, "Control of Communications Security (COMSEC) Material" (reference r), and additional NSA guidance.

g. Conduct an annual physical inspection of all COMSEC products released to non-NATO and non-CCEB nations in support of combatant commands' interoperability requirements, in accordance with NSA/CSS Policy Manual 3-16 (reference r), NSTISSI No. 4005, "Safeguarding Communications Security (COMSEC) Facilities and Materials" (reference s), NAG-14C, "Safeguarding COMSEC Material and Facilities" (reference t), and NAG-18A, "Allied COMSEC Material Accounting Manual" (reference u) and Article IX of a signed CIS MOA or paragraph 5 of a signed IEA.

h. Certify, or coordinate certification, of foreign INFOSEC facilities located in non-NATO countries in accordance with NAG-14C (reference t).

3. Military Services and Departments, Their International Program Offices (IPOs), Defense Security Cooperation Agency (DSCA), and Security Assistance Officers will:

a. Support combatant commands in planning and establishing FMS case(s) for site surveys to identify interoperability requirements that may drive the foreign release of COMSEC products or associated COMSEC information.

b. Participate in site surveys with the combatant commands and foreign nation.

c. Coordinate with the combatant commands for any activity related to the foreign sale of military articles that may contain or require COMSEC products or associated COMSEC information.

d. For COMSEC releases that are relevant to multiple combatant commands, notify and coordinate with all commands involved to submit any CRRs to the Joint Staff and the DIRNSA in accordance with this instruction.

e. Ensure appropriate international agreements (IAs) and RIPs/RISs are in place before COMSEC products are discussed or released to foreign partners (see Enclosure A, paragraph 7). This is especially important in large cooperative development efforts involving multiple countries.

f. Prior to offering any letter of offer and acceptance (LOA) that may include COMSEC products, the implementing agency must forward a letter of request (LOR) to NSA's Office of International Transactions requesting validation of COMSEC release approvals for the interoperability requirement that the release supports and authorization to include a COMSEC product on a service LOA. The DIRNSA may not delegate sales of S-Type equipment to other implementing agencies, in which case the DIRNSA will take the LOR for action to develop an LOA.

g. DSCA will identify the implementing agency responsible for preparing any FMS-CDS case to satisfy U.S. interoperability requirements and inform the combatant command.

h. Prepare FMS-CDS cases for COMSEC products and associated COMSEC information.

i. Identify funding and/or contractual mechanism(s) for COMSEC custodians of NSA COMSEC accounts that support a signed CIS MOA.

j. DSCA and all implementing agencies must ensure the restrictions identified on RISs are clearly conveyed to the purchasing foreign partner. In particular the stipulation that non-NATO and non-CCEB nations will not retain title to COMSEC equipment and the U.S. has a right to recall it at any time.

4. DIRNSA (in accordance with DODD 5100.20, "National Security Agency/Central Security Service (NSA/CSS)" (reference v), and DODI 8523.01 (reference a)) will:

a. Review Joint Staff validated CRRs and identify the appropriate COMSEC solution to support the combined interoperability requirement.

b. Forward the Joint Staff validated CRR and the identified solution to the CNSS Secretariat or national manager for approval, as required by NSTISSP-8 (reference b).

c. In the event that a COMSEC solution is not available to meet the validated interoperability requirement due to a technology gap or a specific security concern; NSA will notify the Joint Staff. The Joint Staff will forward a formal response to the requesting combatant command. The combatant command can work with NSA to determine an alternate solution, and may alter the nature of the requirement, provide sufficient justification to support the original requirement to overcome the security concerns, or withdraw the proposed interoperability requirement. In the event that NSA provides an estimated timeline for when a COMSEC solution may become available, and the combatant command elects to wait until the solution exists, a new CRR

shall be submitted. If the interoperability requirement has not changed, the Joint Staff will authorize the combatant command to submit the CRR directly to the DIRNSA.

d. Upon CRR approval, release a COMSEC RIP or RIS notification message.

e. Review and approve the COMSEC products and services portion of CIS MOAs, and delegate, through the Joint Staff to the combatant command, the authority to negotiate and conclude a CIS MOA.

f. Review and approve IEAs, and delegate to the combatant command the authority to negotiate and conclude an IEA.

g. Support the combatant command's request to establish an NSA COMSEC account under the terms of a CIS MOA, by providing:

(1) A unique account number that identifies the COMSEC account as one governed by NSA COMSEC accounting regulations.

(2) Copies of NSA COMSEC accounting manuals (NSA/CSS Policy Manual 3-16 (reference r), NAG-14C (reference t), and NAG-18A (reference u)) and associated accounting software.

(3) COMSEC custodian training for the U.S. custodian and alternate U.S. custodian.

(4) Guidance to the combatant command on performing COMSEC account audits.

(5) Formally recognize and approve the use of other formally established COMSEC accounts for the purpose of controlling U.S. crypto-material.

h. Maintain records of all COMSEC products or associated COMSEC information transferred to foreign nations.

i. Oversee the development of special purpose (S-type) equipment(s) to meet non-NATO and non-CCEB nation interoperability requirements.

j. Prepare FMS-CDS cases for COMSEC products and associated COMSEC information, and maintain a consolidated record of FMS-CDS cases.

k. Authorize the Services, under specific circumstances, to prepare FMS-CDS cases for COMSEC products and associated COMSEC information.

l. Review and approve combatant command or Service-sponsored ship rider requests.

m. Provide policy guidance for cryptographic modernization programs to ensure that U.S. stated and defined interoperability requirements continue without loss of operational effectiveness. Ensure that adequate policy guidance covers consortiums for critical elements to tactical data-link networks and emerging communication technologies. (i.e., MIDS terminals and software defined radios).

5. Defense Information Systems Agency (DISA) will:

a. Review and approve the CM portion of CIS MOAs.

b. Support the combatant command's CCIB process, to include providing a representative at CCIBs who will be responsible for developing, testing, and maintaining information standards for use by C4I systems in combined operations. The DISA representative will serve as the U.S. Head of Delegation (HOD) and, as such, will be responsible for gaining and coordinating U.S. positions and drafting the U.S. Guidance Package in accordance with the following: CJCSI 2700.01C, "International Military Agreements for Rationalization, Standardization, and Interoperability Between the United States, Its Allies, and Other Friendly Nations" (reference w); CJCSI 6010.01D, "Coordination of United States Command, Control, Communications, and Computer Systems Positions in International Forums" (reference x); and CJCSI 6610.01C, "Tactical Data Link Standardization Implementation Plan" (reference y).

ENCLOSURE C

PROCEDURES FOR A COMSEC RELEASE REQUEST (CRR)

1. General. Combatant command strategic planning, which includes allied and coalition interoperability requirements, drives C4I procurements and COMSEC releases. The COMSEC release process is designed to support combatant command combined interoperability requirements without compromising U.S. security or degrading the U.S. COMSEC posture.

2. Detailed COMSEC Release Procedures. A block diagram of the COMSEC release process is detailed below in Figure C-1. Each numbered step in Figure C-1 is discussed in detail in the following paragraphs.

a. Step One -- Combatant Command Interoperability Requirement. Combatant command identifies a COMSEC interoperability requirement (CIR) that requires the release of COMSEC products or associated COMSEC information to a foreign nation. The release must be consistent with the criteria in paragraph 1 and the limitations in Enclosure A, paragraph 2 of this instruction.

b. Step Two -- COMSEC Release Request Type. The combatant command identifies the type of release required to meet the identified interoperability requirement.

(1) Step Two Alpha -- Release in Specific (RIS). Utilized when a defined set (quantity and recommended nomenclature) of COMSEC products in support of the identified interoperability requirement is known. For RIS requests, the combatant command determines the appropriate bilateral agreement and initiates actions to negotiate and conclude an IA as outlined in Enclosure C, Appendix B (CIS MOA) or Appendix C (IEA). (NOTE: A signed CIS MOA may support multiple RIS approvals as appendixes to the CIS MOA's Annex B. An IEA, however, may only support one specific interoperability requirement. If subsequent requirements are determined, then the combatant command must generate a new IEA.)

(2) Step Two Bravo -- Release in Principle (RIP). Utilized when a detailed discussion of COMSEC products/information with the foreign nation is required to develop a COMSEC solution to meet the identified interoperability requirement. A RIP does not require negotiation of a bilateral agreement.

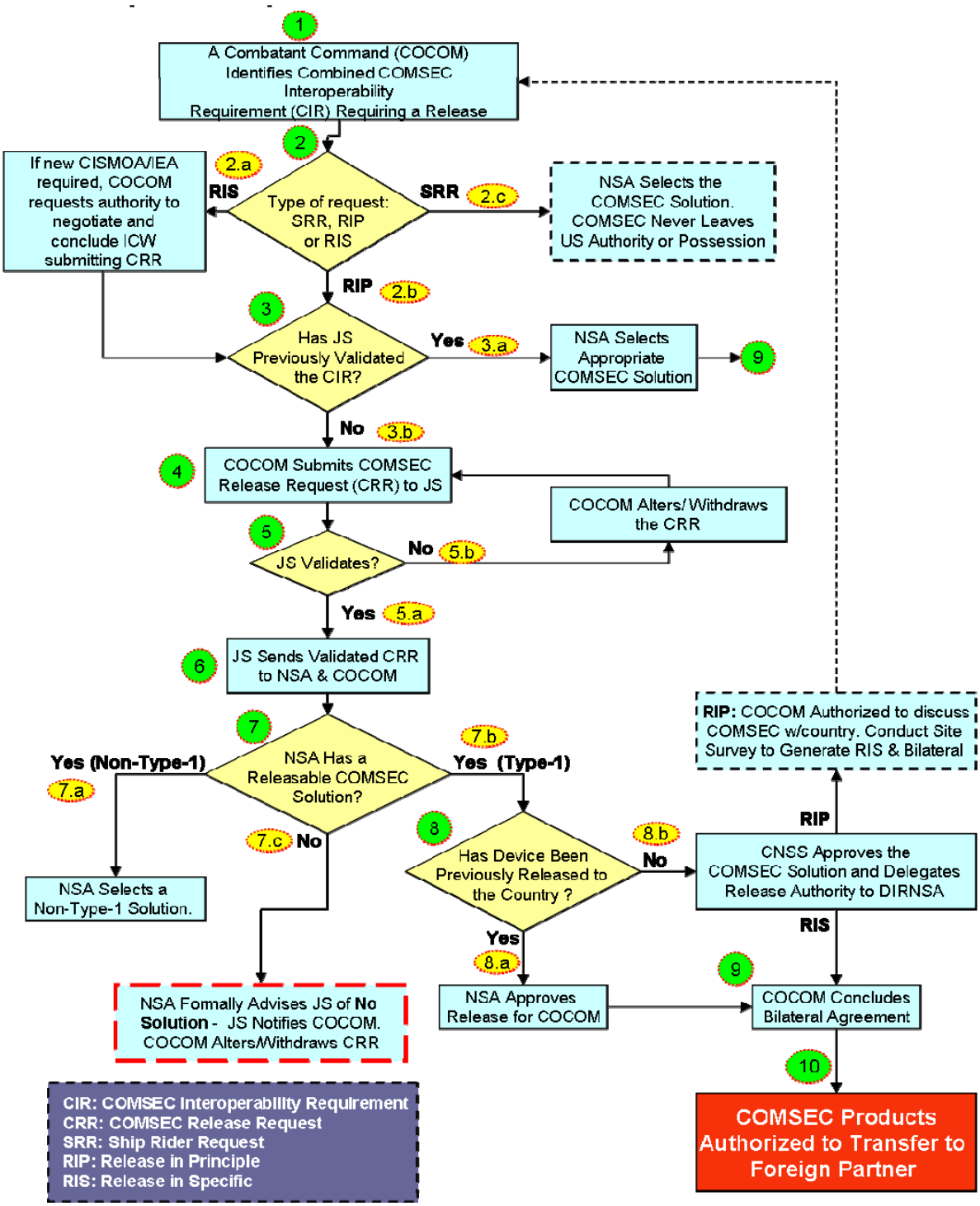

Figure C-1. COMSEC Release Procedures Overview

(3) Step Two Charlie -- Ship Rider Request (SRR). Utilized to solve a temporary interoperability requirement for combined operations or exercises. An SRR is not an actual release of COMSEC products or associated information to a foreign partner. An SRR is sent directly to the DIRNSA for determination of a COMSEC solution and does not require negotiation of a bilateral agreement.

c. Step Three -- CRR Validation Status. The Combatant command determines the correct routing path for the CRR as follows:

(1) Step Three Alpha -- Interoperability Requirement Previously Validated. Combatant command should submit a CRR directly to the DIRNSA and include the Joint Staff as an INFO addressee. The combatant command should first confirm with the Joint Staff that revalidation is not required. Revalidation will be required if the location, network, quantity or type of COMSEC devices significantly differs from the previously approved release or the interoperability requirement changes from the previous validation.

(2) Step Three Bravo -- Interoperability Requirement Not Previously Validated or Changed Significantly from Previous Validation. Combatant command should submit a CRR to the Joint Staff for validation.

d. Step Four -- Combatant Command CRR submitted to the Joint Staff. The Joint Staff will begin the validation process and coordinate the request with the appropriate joint directorates and agencies.

e. Step Five -- Validation. The Joint Staff completes the validation process and proceeds as follows:

(1) Step Five Alpha -- CRR Validated by Joint Staff. The Joint Staff validates the combatant command interoperability requirement.

(2) Step Five Bravo -- CRR Not Validated by Joint Staff. The Joint Staff does not validate the combatant command interoperability requirement and notifies the combatant command. The combatant command shall elect to alter the nature of the requirement, provide sufficient justification to support the original requirement, or withdraw the proposed interoperability requirement.

f. Step Six -- Joint Staff Forwards Validation. The Joint Staff will forward the validated CRR to the DIRNSA and notify the combatant command.

g. Step Seven -- DIRNSA Determines COMSEC Solution. The DIRNSA will determine which of the following COMSEC solution exists:

(1) Step Seven Alpha -- Non-Type-1 Solution. The DIRNSA determines that a non-Type-1 solution should be utilized to support the combatant command interoperability requirement.

(2) Step Seven Bravo -- Type-1 Solution. The DIRNSA determines that a Type-1 solution should be utilized to support the combatant command interoperability requirement. Proceed to Step Eight.

(3) Step Seven Charlie -- No Appropriate Solution. The DIRNSA determines and formally advises the combatant command via the Joint Staff that no appropriate solution exists to support the interoperability requirement. The combatant command can work with NSA to determine an alternate solution, and may alter the nature of the requirement, provide sufficient justification to support the original requirement to overcome the security concerns, or withdraw the proposed interoperability requirement. In the event that NSA provides an estimated timeline for when a COMSEC solution may become available and the combatant command elects to wait until the solution exists, a new CRR shall be submitted (Step Four). If the interoperability requirement has not changed, the Joint Staff will authorize the combatant command to submit the CRR directly to the DIRNSA (Step Seven).

h. Step Eight -- Release Approval Determination. The DIRNSA pursues release approval for Type-1 COMSEC solutions as follows:

(1) Step Eight Alpha -- DIRNSA Release Approval. If the COMSEC device has been previously released to the foreign partner, then the DIRNSA is authorized as the National Manager to approve the release. The DIRNSA will formally notify the combatant command of release approval.

(2) Step Eight Bravo -- CNSS Release Approval. If the COMSEC device has not been previously released to the foreign partner, then a CNSS release approval is required. Following the CNSS approval of the COMSEC solution, the CNSS will delegate release authority to the DIRNSA. The DIRNSA will formally notify the combatant command of release approval. If the CNSS does not approve the release, the DIRNSA will provide feedback/rationale for the CNSS disapproval to the Joint Staff and the combatant command. The combatant command may elect to alter and resubmit a new CRR that addresses/mitigates the CNSS reason(s) for disapproval.

(a) For RIP approvals, combatant command initiates a requirements survey with the foreign nation. The combatant command sponsors a requirements survey to discuss the interoperability requirement with the foreign nation and to develop specific COMSEC requirements that support a RIS request. The requirements survey team may include representation from NSA, DSCA, Service IPO, Security Assistance Office (SAO), or Defense Attaché (DATT) and other organizations as appropriate. The combatant command may request that a FMS case be established to support the site survey. Once the combatant command has identified the exact number and type of COMSEC products required (as a result of the requirements survey), the combatant command shall submit another CRR requesting RIS approval (Step One). The RIP will also allow for an open discussion of operational interoperability requirements during the CCIB and thereby lead to further refinement of number and type of COMSEC products required.

(b) For RIS approvals, proceed to Step Nine.

i. Step Nine -- Combatant Command Concludes Bilateral Agreement. For RIS approvals, combatant command initiates action to negotiate and conclude the appropriate bilateral agreement (CIS MOA or IEA). COMSEC products or associated COMSEC information shall not be physically transferred until a bilateral agreement is signed.

j. Step Ten -- Transfer of COMSEC Products. In accordance with the terms of the bilateral agreement, COMSEC products and associated COMSEC information may be transferred to the foreign nation.

3. COMSEC RELEASE REQUEST (CRR) Message Format Details. The CRR message format is detailed below. The CRR message and individual paragraphs should be classified in accordance with NSTISSI No. 4002, Annex B, "Classification Guide for COMSEC Information" (reference z). A CRR example can be found in Enclosure C, Appendix A of the present document.

a. Message Addressees -- Combatant commands will address CRRs to the Joint Staff (JOINT STAFF WASHINGTON DC//) and provide an info copy to DIRNSA (DIRNSA FT GEORGE G MEADE MD//DP2//). As previously stated, Joint Staff, NSA, and COCOM POCs change too frequently to list in this instruction. Therefore, it is the responsibility of the coordinating parties to update e-mail addresses between POCs to ensure the CRRs arrive at the right office for processing. Additionally, to ensure proper coordination between the operational community and the security assistance community, the following INFO addressees will be included on all CRR messages:

SECDEF WASHINGTON DC//USDP:DSCA/USDP:ISA/DTSA//
CNO WASHINGTON DC//N2N6F1//
NAVY IPO WASHINGTON DC//02//
DA WASHINGTON DC//DUSA-IA//
OSAF WASHINGTON DC//IA//
USASAC ALEXANDRIA VA//AMSAC//

b. Subject Line. The acronym CRR will be included in the SUBJECT line. The phrase "Cross-Command" will be included in the SUBJECT line for cross-command requirements/requests. Previous releases (RIP or RIS) of the COMSEC device (DIRNSA release message) should be listed as references.

c. Body Paragraph 1 -- Interoperability Requirement. Identify the type of CRR: RIP or RIS. Describe the combatant command's foreign interoperability requirement: Attempt to answer who, what, when, where, and why the interoperability requirement will be executed in support of an initiative/ operations plan/exercise. For cross-command requirements, the combatant command submitting the message (the supported or "gaining" combatant command) must acknowledge that it has coordinated the request with all affected combatant commands, and must list points of contact (phone and e-mail).

d. Body Paragraph 2 -- COMSEC Product Needs. Combatant commands should focus on the required capabilities the COMSEC solution must provide, not on a specific COMSEC product. A combatant command may request a specific COMSEC product; however, submission of this request does not guarantee release of the specifically requested IA products or information.

(1) Identify any COMSEC/communications products that do not perform well in theater or on a specific platform, based on the combatant command's experience or information provided by the program manager of a weapons platform.

(2) Identify number/location of operational COMSEC products required. Provide as much detail as possible regarding exact physical location, platforms, and anticipated users (if available, provide network architecture diagram). In addition, specify configuration management details for each device (U.S., NATO, Coalition) with which requested products shall interoperate.

(3) Identify specific COMSEC products that are or will be deployed by U.S. users with which the foreign nation must interoperate. Provide as much

detail as possible regarding interoperability requirement with U.S. COMSEC devices already in use.

(4) Identify all foreign nations that will require interoperability with U.S. systems, including NATO nations and the devices being utilized.

(5) If a particular COMSEC product is requested, include a justification statement outlining the need for that particular solution. Submission of this request does not guarantee release of the specifically requested IA products or information.

e. Body Paragraph 3 -- Secure Communications Link/Network Description. Provide the following information:

(1) What software load and/or capabilities are needed (HAVEQUICK II, SINCGARS, SATCOM, etc.)? What frequency range is needed? What device(s) will be on the U.S. side of the network (e.g., connecting to KG-175B) (include type, series, and software load, if known).

(2) Mode/means of information transmission – voice only, fax, and/or data; landline, mobile, or satellite transmission? If data, Internet Protocol (IP), or asynchronous transfer mode; link or bulk transmission? What is the minimum required data transfer rate?

(3) Classification of U.S. and/or foreign information to be shared via the link/network.

f. Body Paragraph 4 -- Key Management Plan. Provide an overview of lifecycle management for keying material. [NOTE: Some information may depend on the specific COMSEC product that the DIRNSA recommends, in which case NSA will work with the combatant command to identify that information.

(1) Identify desired key 'net configuration' – common net, separate point-to-point links, etc.

(2) Identify desired quantity of key required at each node/location: will some nodes/locations require multiple short titles to support separate point-to-point links?

(3) Identify the office and/or organization responsible for ordering new and/or existing key, and for approving or managing its use (i.e., controlling or command authority and user representatives).

(4) Identify procedures for key distribution, re-key and compromise recovery.

(5) Identify if a multinational solution and key are required and include the list of nations/alliance partners.

g. Body Paragraph 5 -- Bilateral Agreement. Identify the bilateral agreements that will support the transfer of COMSEC products and associated COMSEC information. If no agreement exists, outline a plan to negotiate and conclude.

h. Body Paragraph 6 -- COMSEC Procurement/Accounting Mechanism. Identify the COMSEC transfer mechanism (e.g., DCS, FMS, FMS-CDS, or COMSEC equipment loan) and expected timeline of **procurement**. Identify the COMSEC account, POC, and shipping information that will support the proposed COMSEC release. For releases to be supported by a CIS MOA, identify the existing or planned COMSEC account that will safeguard the COMSEC products.

i. Body Paragraph 7 -- Timeline for Requirement. Provide the following information:

(1) Identify expected timeline of **deployment**.

(2) Desired in-place date for COMSEC products and services including key material.

(3) Estimated duration of the requirement for COMSEC products and services to remain in foreign custody.

(4) Identify plans for retrieving released COMSEC products upon conclusion of the operation/exercise.

j. Body Paragraph 8 -- Combatant Command POC. Provide the name, organization, phone number and secure e-mail or fax for the combatant command POC.

k. Body Paragraph 9 -- Additional Remarks. Insert additional pertinent information.

4. Intelligence, Surveillance, and Reconnaissance (ISR) Related COMSEC Releases. ISR related COMSEC releases require additional coordination to ensure timely and accurate processing. As a result, the combatant command should attempt to identify any release requests or aspects of a release request that involve ISR-related capabilities. The goal of the process below is to ensure that ISR-related concerns are identified and addressed at the earliest point in the CRR process.

a. If the combatant command assesses that a possible ISR-related relationship exists, they will address the following additional areas in the applicable sections of the release request:

(1) Collateral ISR Capabilities Related to the COMSEC Release

(2) Multilateral Security Controls

(3) Site Security Surveys

(4) Loss Contingency/Recovery Measures

(5) Handling Procedures

b. In addition to the standard joint directorate coordination during the validation process, coordination with Joint Staff J25 and any additional U.S. government SIGINT/ISR community representatives will be conducted for ISR-related COMSEC device validation requests.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE C

CRR MESSAGE EXAMPLE

DTG
FM COCOM
TO JOINT STAFF WASHINGTON DC//
INFO DIRNSA FT MEADE MD//DP2//
SECDEF WASHINGTON DC//USDP:DSCA/USDP:ISA/DTSA//
CNO WASHINGTON DC//N2N6F1//
NAVY IPO WASHINGTON DC//02//
DA WASHINGTON DC//DUSA-IA//
OSAF WASHINGTON DC//IA//
USASAC ALEXANDRIA VA//AMSAC//
[ADDDITIONAL APPLICABLE OFFICES]
BT
CLASSIFICATION//2202//
MSGID/GENADMIN/[REQUESTING COMMAND/COCOM]//
SUBJ/ CRR RIS (RIP/GR) OF [COMSEC DEVICES/SOLUTION] FOR [INTEROPERABILITY REQUIREMENT] WITH THE GOVERNMENT OF [COUNTRY] IN SUPPORT OF [OPERATION/PLATFORM/ETC...] (CLASSIFICATION)//
REF/A/MSG/COCOM [DTG]//
REF/B/MSG/DIRNSA [DTG]//
REF/C/DOC/CNSS/13FEB97/DOCSN:NSTISSP NO. 8//
REF/D/DOC/CJCS/[DATE OF THIS ISSUANCE]/DOCSN: CJCSI 6510.06B//
NARR/ (CLASSIFICATION) REF A IS A [COCOM] CRR RIP OF [COMSEC DEVICES] FOR [INTEROPERABILITY REQUIREMENT] WITH THE GOVERNMENT OF [COUNTRY] IN SUPPORT OF [OPERATION/PLATFORM/ ETC...]. REF B IS THE DIRNSA APPROVAL FOR THE RIP REQUESTED IN REF A. REF C IS THE NATIONAL POLICY GOVERNING THE RELEASE OF INFOSEC PRODUCTS TO FOREIGN GOVERNMENTS. REF D IS THE CJCS INSTRUCTION THAT ESTABLISHES POLICY AND PROCEDURES FOR RELEASE OF COMSEC INFORMATION AND DEVICES TO FOREIGN GOVERNMENTS.//
POC/LCDR I. M. FLIER, USN, J-6, TEL: DSN XXX-XXX-XXXX, SIPRNET: EMAIL ADDRESS@COCOM.SMIL.MIL//
RMKS//1. (CLASSIFICATION) [COCOM] REQUESTS JOINT STAFF VALIDATION OF THE SECURE INTEROPERABILITY REQUIREMENT FOR THE [RIS/RIP] OF [COMSEC DEVICES] TO THE GOVERNMENT OF [COUNTRY]. **EXAMPLE FOLLOWS**: IN SUPPORT OF CONPLAN XXXX,

[COCOM] HAS A REQUIREMENT TO ESTABLISH A BILATERAL INFORMATION-SHARING NETWORK. THE REQUIREMENT WILL PROVIDE A SECURE NETWORK CONNECTION (**WHAT**) BETWEEN [COCOM] JOINT OPERATIONS CENTER AND [COUNTRY] SENIOR LEADERSHIP (**WHO**) AT COMMAND HEADQUARTERS AND COMBINED OPERATIONS CENTER (**WHERE**) DURING COMBINED AIR AND GROUND OPERATIONS AND EXERCISES (**WHEN**). THE SECURE NETWORK WILL ENSURE SITUATIONAL AWARENESS AND ENHANCE COMMAND AND CONTROL BETWEEN U.S. AND [COUNTRY] FORCES (**WHY**). [COCOM] CONCLUDED AN INFORMATION-SHARING AGREEMENT WITH [COUNTRY] IN [DATE], AUTHORIZING THE EXCHANGE OF [PROGRAM] INFORMATION. AS AUTHORIZED BY THE [RIS/RIP] APPROVAL (REF B), [COCOM] SUBSEQUENTLY DISCUSSED WITH THE GOVERNMENT OF [COUNTRY] POSSIBLE COMSEC SOLUTIONS FOR THIS BILATERAL NETWORK. [COCOM] AND THE GOVERNMENT OF [COUNTRY] HAVE CONCLUDED THOSE DISCUSSIONS AND ARE NOW PREPARED TO MOVE FORWARD WITH IMPLEMENTATION.

2. (CLASSIFICATION) COMSEC PRODUCT NEEDS: [DETAILED TECHNICAL DESCRIPTIONS, IMPACTS, OR INFLUENCES OF THE INTEROPERABILITY REQUIREMENT AND ENVIRONMENT]. INFORMATION DETAILING NODES/LOCATIONS/SYSTEMS/PLATFORMS INVOLVED. QUANTITIES, TO INCLUDE SPARING, REQUIRED FOR EACH NODE/LOCATION/SYSTEM/ PLATFORM:
[HEADQUARTERS, CITY]
[COMBINED OPERATIONS CENTER, CITY]
[SUBORDINATE STAFF DIRECTORATE, CITY]
THESE DEVICES WILL SUPPORT NETWORK ACCESS FROM THE COMBINED OPERATIONS CENTER TO A FORWARD OPERATING LOCATION IN [CITY /COUNTRY]. A NETWORK ARCHITECTURE IS AVAILABLE AND WILL BE EMAILED SEPARATELY. THERE IS A NEED FOR INTEROPERABILITY WITH AN EXISTING NETWORK OF [CRYPTO DEVICES]. THIS NETWORK WILL BE ACCESSED BY U.S. AND [COUNTRY] GOVERNMENT PERSONNEL ONLY.

3. (CLASSIFICATION) SECURE COMMUNICATIONS LINK/NETWORK DESCRIPTION: THE NETWORK WILL BE IP BASED AND UTILIZES THE PUBLIC INTERNET TO INTERCONNECT NODES/SYSTEMS/LANS ETC. LOCATED IN [COUNTRIES/CITIES/ETC]. MINIMIMUM DATA THROUGHPUT IS X MBPS. THE LINK WITH FORWARD LOCATION [X] WILL BE SUPPORTED BY A VSAT LINK, AT A MINIMUM THROUGHPUT OF X MBPS. INFORMATION UP TO THE SECRET//REL TO [COUNTRY] LEVEL WILL BE PASSED OVER THIS NETWORK. SPECIFY CONFIGURATION MANAGEMENT DETAILS FOR ANY AND ALL DEVICES

(U.S., NATO, COALITION) WITH WHICH REQUESTED PRODUCTS SHALL INTER OPERATE.
4. (CLASSIFICATION) KEY MANAGEMENT PLAN: THE XXX WILL SERVE AS THE CONTROLLING AUTHORITY, OR COMMAND AUTHORITY AND/OR USER REPRESENTATIVE FOR THE ABOVE CRYPTONET. IF A KEY IS CURRENTLY BEING USED ON THE NETWORK, PROVIDE SHORT TITLE.
5. (CLASSIFICATION) BILATERAL AGREEMENT: COCOM SIGNED A CIS MOA WITH THE GOVERNMENT OF [COUNTRY] IN [DATE]. EQUIPMENT APPROVED UNDER THIS RIS REQUEST WILL BE DOCUMENTED IN AN APPENDIX TO ANNEX B OF THE CIS MOA.
6. (CLASSIFICATION) COMSEC PROCUREMENT/ACCOUNTING MECHANISM: UPON APPROVAL OF THIS REQUIREMENT, THE [COMSEC DEVICES] WILL BE PROCURED VIA [METHOD OF PROCUREMENT] NO LATER THAN [DATE].
7. (CLASSIFICATION) TIMELINE: [IDENTIFY THE SYSTEM IN-PLACE-DATE AND REQUIRED/PLANNED FOC], AND THEREFORE REQUESTS JOINT STAFF VALIDATION AND IDENTIFICATION AND RELEASE APPROVAL OF APPROPRIATE COMSEC SOLUTIONS. DURATION OF REQUIREMENT WILL BE FOR THE LIFE OF THE INFORMATION-SHARING AGREEMENT, CURRENTLY [# OF YEARS].
8. (CLASSIFICATION) THE COMBATANT COMMAND POINT OF CONTACT FOR THIS REQUIREMENT IS LCDR I. M. FLIER, USN, J-6, TEL: DSN XXX-XXX-XXXX, SIPRNET: EMAIL ADDRESS@COCOM.SMIL.MIL
9. (CLASSIFICATION) ADDITIONAL REMARKS. LIST ANY OTHER PERTINENT INFORMATION.//
BT

* This example serves as a guide for the collection of CRR information needed to obtain a Joint Staff validation and NSA material solution. By using the template, the goal is to expedite the release process; however, the example above may not outline all the information needed to satisfy all requirements. Please provide as much information as possible to assist in making a validation and release decision.

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE C

PROCEDURES AND BOILERPLATE FOR A COMMUNICATION INTEROPERABILITY AND SECURITY MEMORANDUM OF AGREEMENT (CIS MOA)

1. General. The CIS MOA is an international agreement between the U.S. Department of Defense (DOD) and a foreign government Ministry of Defense (MOD) (or equivalent). It provides the legal framework and mechanisms for the long-term transfer and safeguarding of COMSEC products and associated information, and of CM specifications necessary to establish and enhance strategic partnerships, mutual C4ISR endeavors, and interoperability between military forces at the tactical and operational levels. The CIS MOA outlines the responsibilities of the United States in transferring these products and information, and of the foreign nation in using and safeguarding the products and information. If the United States must recall the products, the CIS MOA serves as a record of products transferred to the foreign nation. Finally, the CIS MOA facilitates the creation of a bilateral, multidisciplinary Command and Control Interoperability Board as the forum for managing combined interoperability initiatives.

2. Authority to Negotiate and Conclude. Within the Department of Defense, the authority to negotiate and conclude IAs originates with the Secretary of Defense. DODD 5530.3 (reference f), CJCSI 2300.01D (reference l), and CJCSI 6740.01B (reference m) delegate the authority in separate areas of cognizance to the Secretaries of the Military Departments, certain Under or Assistant Secretaries of Defense, the Chairman of the Joint Chiefs of Staff, and Directors of Defense agencies. Delegation of authority for the CIS MOA rests with the Joint Staff and the DIRNSA, as outlined below:

a. Configuration Management. The Chairman has been delegated the authority to negotiate and conclude international CM agreements. Further delegation to the combatant commands to negotiate and conclude CM IAs is authorized.

b. COMSEC Products and Services. The DIRNSA has been delegated the authority to negotiate and conclude international COMSEC products and services agreements. Further delegation to the combatant commands to negotiate and conclude international COMSEC product and services agreements is authorized.

3. Configuration Management Standards. CM standards are formats for data link interoperability, message texts, and other configuration protocols. The most common standards included in the CIS MOA are U.S. message text format (USMTF), tactical data link (TDL) A, B, J, variable message text format (VMF), data forwarding between data links, standard symbology, joint range extension application protocol (JREAP), and joint multitactical data link operating procedures (JMTOP). Other data standards may be added to the CIS MOA based on Joint Staff validation of the underlying interoperability requirement and concurrence of the DOD executive agent for the particular standard. Adherence to these standards through CM procedures outlined in Annex A to a CIS MOA ensures continued interoperability between U.S. and foreign government military forces. Ongoing management of these standards occurs through the CCIB. Most DOD procedural data standards are unclassified limited distribution. Procedural data standards included in the CIS MOA may be released to a foreign country once the CIS MOA has been concluded. Requests for exception to this policy will be forwarded to DISA's Interface Standards Division, Standards Management Branch (GE332).

4. COMSEC Products and Services Accounting Mechanisms. Under the terms of the CIS MOA, the combatant command and the foreign MOD share responsibility for safeguarding released COMSEC products and associated information in accordance with NAG-14C (reference t) and NAG-18A (reference u) and other amplifying procedures that may be prescribed by USG authorities. The CIS MOA must further state that a COMSEC account, staffed by U.S. citizens and managed under the DIRNSA COMSEC accounting regulations, must account for all COMSEC products and associated information transferred to the foreign nation. Combatant command and the DIRNSA responsibilities associated with this account are outlined below in subparagraph 4.b.

a. CIS MOA COMSEC Account Models. The combatant command, in coordination with its foreign partner(s), shall determine which of the following account models would best support its requirements.

(1) Dedicated Bilateral COMSEC Account. A bilateral COMSEC account supports only one CIS MOA/foreign partner. The account is typically located within the foreign nation and funded solely by the foreign partner through FMS channels.

(2) Regional COMSEC Account. A regional COMSEC account may support multiple CIS MOAs/foreign partners. The account may be co-located

with the combatant command headquarters, or at another U.S. facility that serves as a transportation "hub" within the combatant command's AOR. The combatant command may choose to fund the account itself, or it may rely on proportional funding by its foreign partners through FMS channels. A regional COMSEC account may be a cost-effective mechanism for supporting foreign partners that either cannot afford a dedicated bilateral COMSEC account or do not deem their inventory of released U.S. COMSEC products merits one.

(3) International Organization. Make use of a formally established and recognized COMSEC account established by an international organization (e.g., Military Committee Distribution and Accounting Agency on behalf of NATO).

b. CIS MOA COMSEC Account Responsibilities. NSA/CSS Policy Manual 3-16 (reference r) outlines custodial responsibilities for managing NSA COMSEC accounts. These responsibilities include, but are not limited to, performing central receiving, temporary storage, transfer services, and periodic inventories and inspections of all U.S. COMSEC products and associated information (including key material) provided in support of combatant command interoperability requirements. Custodians will also train foreign MOD personnel in the proper custodianship and safeguarding of U.S. COMSEC products and associated information. Because of the unique aspects of establishing and managing an NSA COMSEC account in support of a CIS MOA, the combatant command and NSA will share account responsibilities as outlined below.

(1) DIRNSA Responsibilities. The DIRNSA will serve as the central office of record (COR) for the account in accordance with NSA/CSS Policy Manual 3-16 (reference r); however, COR audit and inventory functions outlined in Section XVII of reference r shall be the responsibility of the combatant command. Upon combatant command request to establish an NSA COMSEC account in support of a CIS MOA, the DIRNSA will provide the following:

(a) A unique account number registering the COMSEC account as one governed by NSA COMSEC accounting regulations.

(b) Copies of NSA COMSEC accounting manuals (NSA/CSS Policy Manual 3-16 (reference r), NAG-14C (reference t), and NAG-18A (reference u) and associated accounting software.

(c) COMSEC custodian training for the custodian and alternate custodian as well as NSA-certified COMSEC audit training as necessary for the combatant commands to perform their duties of the FMS COMSEC accounts.

(d) Guidance to the combatant command on performing COMSEC account audits and inventories.

(e) Advice as the NSA advisor to the U.S. representative and combatant commands in preparation for CCIBs in order to ensure appropriate U.S. policy guidance is effected in coordination with bilateral information exchange agreements.

(2) Combatant Command Responsibilities. The combatant command will oversee the establishment and ongoing management of the account. Specifically, the combatant command will:

(a) Submit a formal request to NSA to establish an NSA COMSEC account under the terms of a CIS MOA.

(b) Identify funding mechanism(s) to support travel costs associated with periodic inspections/audits of the account, COMSEC products in the account, and facility certification. Depending on the type of COMSEC account established (bilateral vs. regional), the combatant command may request that the foreign nation fund an FMS case to support all or part of the costs associated with the account.

(c) Perform periodic audits and semiannual inventories of the account, in accordance with NSA/CSS Policy Manual 3-16 (reference r) and additional DIRNSA guidance.

(d) Direct foreign LORs for a CIS MOA COMSEC account to DSCA via the SAO, for FMS case establishment.

5. Command and Control Interoperability Board. The CCIB, under the terms of the CIS MOA, is normally a bilateral, multidisciplinary forum for addressing combined interoperability initiatives on an annual basis. The CCIB should be governed by a terms of reference (TOR) document that identifies its mission, composition, responsibilities, and method of work.

a. CCIB Responsibilities. The specific responsibilities of the CCIB include, but are not limited to, the following:

(1) Determining new combined interoperability requirements and discuss new requests.

(2) Developing and maintaining standards, procedures and information to be exchanged in support of interoperability requirements.

(3) Determining appropriate training.

(4) Overseeing implementation and lifecycle support, including combined testing and training, for interoperability requirements and CM.

b. U.S. Representation at CCIBs. The combatant command is responsible for ensuring appropriate participation from the Services and DOD agencies at CCIBs. The senior combatant command representative serves as the CCIB co-chair, with the senior foreign partner representative serving as the other co-chair. DISA's Combined Interoperability Program (CIP) team provides the U.S. representative in CCIBs responsible for the development, testing, and maintenance of information standards for use by C4I systems in combined operations. Additionally, DISA provides technical support, as directed by the Chairman or ASD(NII), to CCIBs or to U.S. representatives to the CCIB. The DISA representative will serve as the U.S. HOD, with responsibility for gaining and coordinating U.S. positions and writing the U.S. Guidance Package in accordance with CJCSI 2700.01C (reference w), CJCSI 6010.01D (reference x), and CJCSI 6610.01C (reference y).

6. COMSEC Device Release Documentation. The combatant command shall document all transferred COMSEC products in appendixes to Annex B of the CIS MOA.

a. Each appendix of the CIS MOA shall include, at a minimum:

(1) COMSEC product nomenclature, quantity and serial number.

(2) Brief description of the interoperability requirement that the COMSEC products support. (NOTE: This shall include the DIRNSA release approval message DTG.) It is not appropriate to include the actual CRR or other internal USG coordination documentation in Annex B. Spreadsheet and lists that include the required information about a release are acceptable.

(3) Procedures for return of COMSEC products upon termination of interoperability requirement.

(4) For COMSEC products transferred via FMS-CDS channels, the equipment list included with the LOA.

b. The following limitations/restrictions are imposed on approved COMSEC product/equipment releases:

(1) The United States will retain title/ownership of the COMSEC equipment.

(2) The COMSEC equipment will be subject to recall by the United States at any time.

(3) The COMSEC equipment will be used only on the circuits for which the release was requested and approved.

(4) The COMSEC equipment will be installed, configured, and maintained only by properly qualified and authorized U.S. personnel.

(5) The COMSEC equipment and associated information will not be exposed to citizens of a third country without the prior and express approval of appropriate U.S. authorities.

(6) Only U.S.-produced keying material will be used to key the COMSEC equipment.

(7) While in foreign custody, the COMSEC equipment and associated information will be afforded physical protection commensurate with U.S. standards.

(8) U.S. authorities will be notified in a timely manner of the compromise of the COMSEC equipment or associated information.

(9) Foreign nationals will not be afforded or authorized access to the cryptographic logic of the COMSEC equipment.

c. If additional quantities of a previously released COMSEC product are transferred to support an existing requirement, the appendix corresponding to the original requirement/release will be updated to reflect the new quantity. COMSEC products released prior to the conclusion of a CIS MOA, or previously

documented in a separate COMSEC MOU, will also be documented in separate appendixes.

d. The combatant command may choose to append a signed LOA to Annex B of the CIS MOA rather than develop a separate appendix. The combatant command must coordinate with NSA/DP2 and DSCA to insert into the LOA-specific information about the interoperability requirement, release approval, and unique product handling/accountability requirements. The DIRNSA will advise the delegated implementing agency on specific limitations to the product transfer in the authorization letter. DSCA will ensure LOAs include appropriate language.

7. Detailed CIS MOA Preparation Procedures. The following paragraphs describe the steps in preparing, negotiating and concluding a CIS MOA. Figure C-B-1, below is a block diagram of the CIS MOA procedures.

a. Step One -- Combatant Command Interoperability Requirement. The combatant command identifies a requirement to pursue negotiation of a CIS MOA in support of foreign interoperability requirements. The combatant command can pursue the CIS MOA process in tandem with the CRR process.

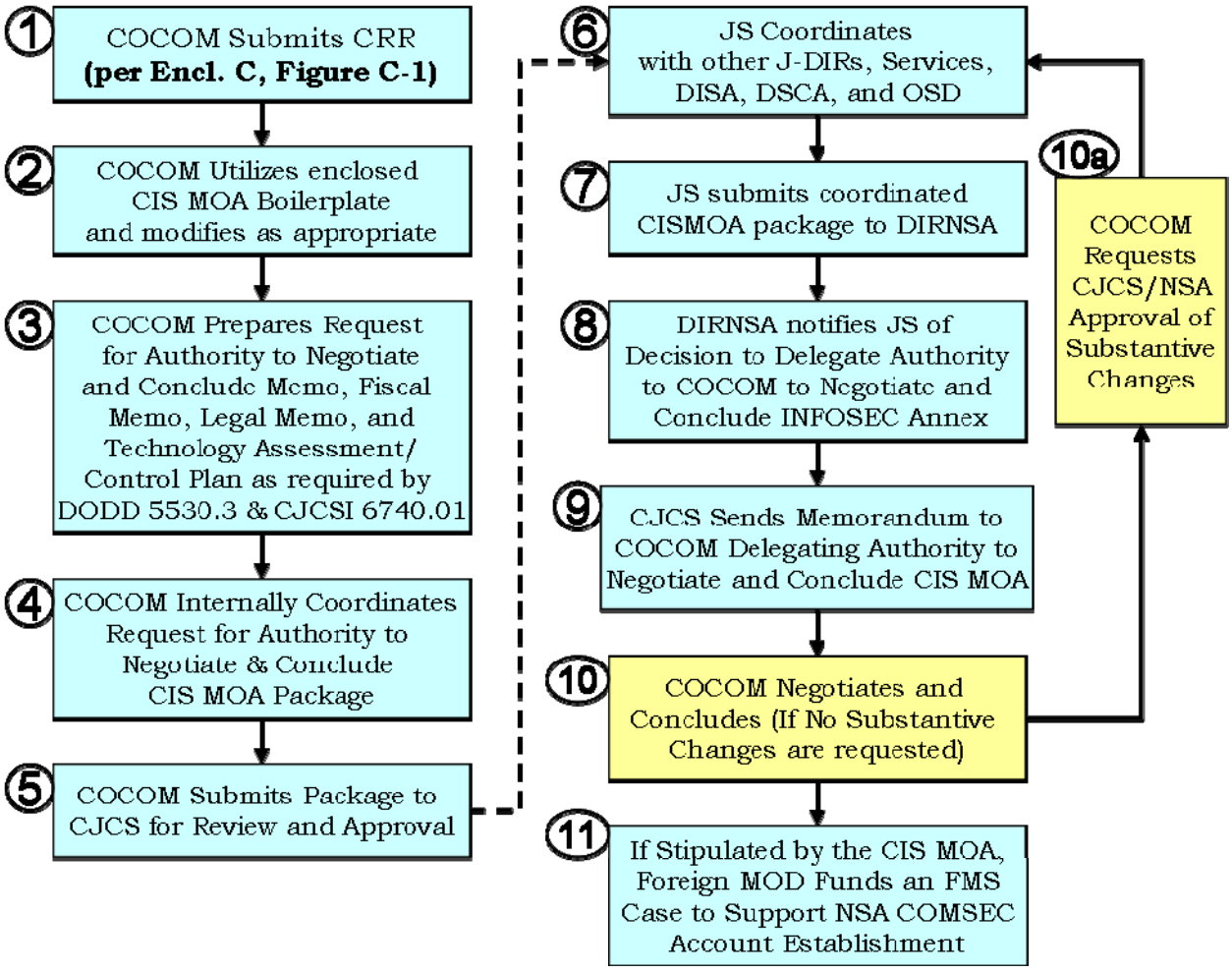

Figure C-B-1. CIS MOA Preparation Procedures

b. Step Two -- Utilize Current Boilerplate CIS MOA. Figure C-3 is the current Joint Staff, DIRNSA boilerplate CIS MOA.

(1) The combatant command should replace all references in the boilerplate document to reflect the specific foreign nation and MOD that will enter into the agreement. The combatant command should also appropriately classify the agreement. The language in the boilerplate CIS MOA has been approved by the Joint Staff, DIRNSA, and DISA, and it represents the consolidated U.S. position relating to COMSEC and CM agreements with foreign countries. However, the combatant command should modify the boilerplate language to accommodate particular aspects of a bilateral relationship, such as previous bilateral agreements, the need (or lack thereof)

for a CCIB, and the foreign nation's responsibility to fund the CIS MOA COMSEC account. With respect to previous COMSEC agreements, Article XIII in the boilerplate document includes specific language required to subsume previous agreements into the CIS MOA. Reference to these agreements should be documented in Annex B of the CIS MOA. Should the United States have no previous COMSEC agreements with a country, Article XIII may be removed from the CIS MOA.

(2) Any substantive deviations from this boilerplate document must be approved by Joint Staff, Joint Staff Legal Counsel, and the DIRNSA.

c. Step Three -- Prepare CIS MOA Staffing Package. In addition to the draft CIS MOA text, DODD 5530.3 (reference f) and CJCSI 6740.01B (reference m) require the combatant command to submit the three support documents detailed below. Additional information describing the three documents is contained in reference f.

(1) Legal Memorandum. Specifically identifies the constitutional, statutory, treaty, or other legal authority that authorizes the United States to undertake each obligation and to receive each benefit and any other relevant legal considerations in the proposed agreement.

(2) Fiscal Memorandum. Provides the estimated cost, by fiscal year, to each participant to undertake all proposed project obligations, the source of obligation funding or, if all funds are not presently available or programmed for out years, an explanation of any plan to obtain additional funds or legislative funding authority. Computations for exchanges of equivalent value and the method for determining value also should be included.

(3) Technology Assessment/Control Plan (TA/CP). Describes the scope of the agreement and identifies the technologies and sensitive information involved, evaluates the foreign technologies or other benefits the United States is likely to acquire, assesses the risk to U.S. information, establishes foreign disclosure guidance, and prescribes specific requirements for the protection of sensitive and classified technical information during the course of the agreement. (See reference f, Enclosure 7 for TA/CP guidance.)

d. Step Four -- Internally Coordinate Request for Authority to Negotiate and Conclude CIS MOA Package. Combatant command prepares a memorandum to the Chairman requesting authority to negotiate and conclude a CIS MOA agreement. The combatant command staff coordinates a command

memorandum, draft CIS MOA, fiscal memorandum, legal memorandum, and TA/CP. After coordination is concluded, the combatant command commander signs the memorandum to the Chairman.

e. Step Five -- Submit CIS MOA Package to CJCS for Approval. The combatant command sends the CIS MOA package, with signed request for authority to negotiate and conclude, to the Joint Staff.

f. Step Six -- Joint Staff Coordinates Draft CIS MOA. The Joint Staff sends the draft CIS MOA package to Joint Staff directorates, Joint Staff Legal Counsel, Services, DISA, DSCA, and OSD for comments and concurrence.

g. Step Seven -- The Joint Staff submits the coordinated CIS MOA package to the DIRNSA. Requests delegation authority for the COMSEC portion of the CIS MOA.

h. Step Eight -- DIRNSA Delegates to Combatant Command, through the Chairman, Authority to Negotiate and Conclude. After reviewing the draft CIS MOA, DIRNSA notifies the Chairman that the combatant command is authorized to negotiate and conclude the COMSEC portion of the CIS MOA. If DIRNSA identifies any substantive changes, it passes those changes to the Joint Staff and the combatant command staff to resolve.

i. Step Nine -- CJCS Sends Memorandum to Combatant Command Delegating Final Authority to Negotiate and Conclude the CIS MOA. After coordination is complete and delegation authority is received from DIRNSA, the Director, Joint Staff (DJS) sends a memorandum on behalf of the Chairman to the combatant command delegating authority to negotiate and conclude the CIS MOA. Any changes to the draft CIS MOA are noted in the DJS memorandum. The DJS memorandum requires the combatant command to resubmit the CIS MOA for review prior to conclusion if any substantive changes are made during negotiations.

j. Step Ten -- Combatant Command Negotiates and Concludes CIS MOA. After receiving CJCS delegation authority, the combatant command may provide the foreign government with a copy of the draft CIS MOA before negotiations. Generally, the combatant command provides the CIS MOA to the DATT or the SAO at the American embassy, and the DATT or SAO provides a copy to the foreign government MOD. The combatant command tailors a negotiation team with representation from DISA, NSA, and DSCA as required. During the negotiation phase, the combatant command should explain the

requirement for a CIS MOA COMSEC account and the foreign MOD's responsibilities to fund the account. The combatant command should provide the foreign MOD with copies of NAG-14C (reference t) and NAG-18A (reference u), which outline specific COMSEC accountability requirements including the requirement for a COMSEC facility. If the foreign government MOD proposes no substantive changes to the draft CIS MOA, the combatant command may conclude the CIS MOA. After the CIS MOA is signed, reproducible copies are provided by the combatant command to the General Counsel of the Department of Defense (Washington, D.C. 20301-1600), NSA Information Assurance Operations Group (DP2), DISA legal counsel, DSCA, and the Joint Staff.

k. Step Ten Alpha -- Substantive Changes are proposed. The combatant command staff and Legal Counsel review the proposed substantive changes. The combatant command submits proposed substantive changes with combatant command recommendations to the Chairman for review and coordination. After coordination is complete and delegation authority is received from DIRNSA, the DJS sends a memorandum on behalf of the Chairman to the combatant command delegating authority to negotiate and conclude the CIS MOA. The combatant command then negotiates the approved changes and concludes the agreement.

l. Step Eleven -- COMSEC Accounting Mechanism Established. In accordance with the signed CIS MOA, the combatant command establishes the NSA-recognized COMSEC account to support the safeguarding of released U.S. COMSEC products and associated information. If the CIS MOA requires foreign MOD funding to support the account, the foreign nation must submit an LOR through the U.S. SAO to DSCA for FMS case establishment. Once the COMSEC account is approved, funded, and staffed, COMSEC products and information may be transferred to the foreign nation.

8. Relocation of COMSEC Products. Temporary equipment transfers (TET) and temporary relocation of COMSEC products must be approved by the combatant command before taking place. Because COMSEC products are released to support specific requirements in a specific location, the combatant command must determine whether temporary relocation is justified. Permanent *relocation* (movement from one location to another) of COMSEC products must be approved by the DIRNSA before taking place. Reproducible copies of signed agreements modifying the location of released COMSEC products will be forwarded by the combatant command to DOD General Counsel (Washington, D.C. 20301-1600), DISA legal counsel, DSCA, and the Joint Staff. Message

examples for equipment relocation requests are shown in figures C-B-2 and C-B-3, below.

9. CIS MOA Boilerplate. Figure C-B-4 is the CIS MOA boilerplate. As noted in the figure, some articles or statements shall be considered non-negotiable.

FROM [COCOM COMPONENT]
TO [COCOM]
INFO DIRNSA FT GEORGE G MEADE MD//DP2//
JOINT STAFF WASHINGTON DC//
[ADDITIONAL APPLICABLE OFFICES]
BT
CLASSIFICATION//2202//
MSGID/GENADMIN/[SENDING COMMAND/COCOM COMPONENT]//
SUBJ/TEMPORARY EQUIPMENT TRANSFER (TET) OF [COMSEC DEVICE] [CLASSIFICATION]//
POC/LT R. E. QUEST, USN, N-6, TEL: DSN XXX-XXX-XXXX, SIPRNET: EMAIL ADDRESS@NAVY.SMIL.MIL//
1. (CLASSIFICATION) REQUEST APPROVAL FOR TEMPORARY EQUIPMENT TRANSFER (TET) OF COMSEC EQUIPMENT TO SUPPORT [COCOM] AND [COUNTRY] [EXERCISE].
2. (CLASSIFICATION) REQUEST AUTHORITY TO USE TET FOR [COMSEC DEVICE AND QUANTITY] IN SUPPORT OF [EXERCISE]. CURRENTLY THERE ARE TWO [COMSEC DEVICES] LOCATED AT [LOCATION X], ONE FOR ONLINE USE AND ONE AS A SPARE. REQUEST TO MOVE THE SPARE [COMSEC DEVICE] FROM [LOCATION X TO LOCATION Y] IN SUPPORT OF EXERCISE REQUIREMENTS. BOTH DEVICES ARE UNDER THE U.S./[COUNTRY] CIS MOA, ANNEX XXX.
3. (CLASSIFICATION) THE REQUESTED EFFECTIVE PERIOD FOR EQUIPMENT UTILIZATION IS [BEGIN DATE TO END DATE]. ANY INSTALLATION AND/OR DEINSTALLATION REQUIREMENTS WILL BE COMPLETED OR PERFORMED BY U.S. PERSONNEL.
4. (CLASSIFICATION) REQUEST IMMEDIATE APPROVAL TO ALLOW FOR INSTALLATION AND TESTING OF EQUIPMENT PRIOR TO START OF THE [EXERCISE] ON [DATE].//
BT

Figure C-B-2. Sample Temporary Equipment Transfer (TET) Request

FM [COCOM]
TO DIRNSA FT GEORGE G MEADE MD//I11//
INFO JOINT STAFF WASHINGTON DC//
[COCOM COMPONENT]
[ADDITIONAL APPLICABLE OFFICES]
BT
CLASSIFICATION//2202//
MSGID/GENADMIN/[REQUESTING COMMAND/COCOM]//
SUBJ/[COMSEC DEVICE] EQUIPMENT
RELOCATION[CLASSIFICATION]//
REF/A/DOC/[COCOM] AND [COUNTRY]/[DDMMMYYY]//
REF/B/MSG/[COCOM COMPONENT/[DTG]/[COMSEC DEVICE]
RELOCATION//
POC/LCDR I. M. FLIER, USN, J-6, TEL: DSN XXX-XXX-XXXX, SIPRNET:
EMAIL ADDRESS@COCOM.SMIL.MIL//
NARR/REF A IS THE MEMORANDUM OF AGREEMENT BETWEEN THE
[COCOM] AND [COUNTRY] PERTAINING TO THE PROVISION OF THE
COMMUNICATIONS SECURITY EQUIPMENT SERVICES FOR THE
[COMSEC DEVICE]. REF B IS THE [COCOM COMPONENT] REQUEST
TO RELOCATE [COMSEC DEVICE] EQUIPMENT.//
1. (CLASSIFICATION) REQUEST APPROVAL FOR THE PERMANENT
RELOCATION OF [COMSEC DEVICE] EQUIPMENT TO SUPPORT
CHANGES IN THE EMPLOYMENT OF [COMSEC DEVICE PLATFORM]
FOR [INTEROPERABILITY REQUIREMENT]. [ADDITIONAL REASONING].
2. (CLASSIFICATION) BELOW (IAW REF A) IS THE CURRENT
DISTRIBUTION OF EQUIPMENT TO SUPPORT [INTEROPERABILITY
REQUIREMENT] UNDER THE XXXXXXX ANNEX.

QTY	DEVICE	LOCATION
XXXXXXX	XXXXXXX	XXXXXXX

3. (CLASSIFICATION) BELOW IS THE PROPOSED AND PLANNED
EQUIPMENT REDISTRIBUTION TO SUPPORT [INTEROPERABILITY
REQUIREMENT] UNDER THE XXXXXX ANNNEX.

QTY	DEVICE	LOCATION
XXXXXXX	XXXXXXX	XXXXXXX

4. (CLASSIFICATION) IF APPROVED, THE EQUIPMENT WILL BE
INSTALLED UPON DIRNSA AUTHORIZATION. U.S. PERSONNEL WILL BE
USED TO INSTALL EQUIPMENT.
5. (CLASSIFICATION) REQUEST IMMEDIATE APPROVAL TO ALLOW FOR
RELOCATION OF ASSETS TO SUPPORT MISSION REQUIREMENTS. IF
APPROVED THIS MESSAGE AND THE APPROVAL MESSAGE WILL BE
APPENDED TO XXXXXX ANNEX TO SUPPORT PERMANENT
RELOCATION OF EQUIPMENT.//
BT

Figure C-B-3. Sample Permanent Equipment Relocation Request

(CLASSIFICATION)

MEMORANDUM OF AGREEMENT

BETWEEN
UNITED STATES DEPARTMENT OF DEFENSE
AND
COUNTRY MINISTRY OF DEFENSE
CONCERNING
COMMUNICATIONS INTEROPERABILITY AND SECURITY (C)

ARTICLE I

(X//REL TO USA, XXX) This Memorandum of Agreement (MOA) is entered into between the U.S. Department of Defense (DOD) and the **COUNTRY** Ministry of Defense (MOD), (the Parties), in furtherance of the mutual security interests of the U.S. Government (USG) and the Government of **COUNTRY** (**GOV'TACRONYM**), and to promote communications interoperability and security between their respective Armed Forces.

ARTICLE II

(X//REL TO USA, XXX) The purposes of this MOA are to promote tactical Command, Control, and Communications (C3) systems interoperability between the Armed Forces of the **GOV'TACRONYM** and USG; to define policies relating to Configuration Management (CM) of interoperable communications systems, to include Spread Spectrum Communications Systems, testing thereof, and maintenance of Procedural and Technical Standards; and to provide for Secure Communications interoperability between the Parties through the provision by the DOD of Communications Security (COMSEC) Equipment and Services to the MOD to protect classified and sensitive national security information and data. The specific policies and procedures addressing each Party's responsibilities under this MOA are set forth in the attached Annexes A and B, which form an integral part of this MOA.

ARTICLE III

(U) DOD Financial obligations under this MOA are subject to the availability of funds authorized and appropriated for such purposes.

(COMMENT: This article is non-negotiable.)

Figure C-B-4. CIS MOA Boilerplate (page 1 of 15)

ARTICLE IV

(X//REL TO USA, XXX) The standards and baseline documents identified at Appendix 1 of Annex A to this MOA and changes to those standards and documents which support CM responsibilities outlined in this MOA and in Annex A shall be protected in accordance with the provisions of Annex A.

ARTICLE V

(X//REL TO USA, XXX) The MOD shall bear the cost of reconfiguring its communications systems to achieve or maintain combined U.S./**COUNTRY** Armed Forces interoperability. Each Party shall bear its own costs of participating in combined testing, as agreed, with each Party being responsible for the costs associated with its portion of the testing. The MOD shall obtain from the DOD through Foreign Military Sales (FMS) procedures any testing assistance it requires.

(COMMENT: This is negotiable under certain circumstances, however, NSA will not fund.)

ARTICLE VI

(X//REL TO USA, XXX) Subject to USG release approvals, the DOD will provide DOD COMSEC equipment, keying and other materials, and support services to the MOD in order to satisfy requirements for secure interoperability between U.S. and **COUNTRY** Armed Forces through one or more of the following means as mutually agreed:

a. (U) FMS procedures shall be used to provide, by sale or lease, COMSEC equipment, keying and other materials, or support services. Procurement through FMS procedures shall be pursuant to Letters of Offer and Acceptance (LOA) and in accordance with the Arms Export Control Act. In the event of any inconsistency between an LOA and this MOA, the LOA shall take precedence.

b. (U) Other authorized means, as determined by DOD, may be used to provide COMSEC equipment or materials including keying materials, in order to satisfy short-term DOD/MOD secure interoperability requirements.

(COMMENT: This article is non-negotiable.)

Figure C-B-4. CIS MOA Boilerplate (page 2 of 15)

ARTICLE VII

7.1 (X//REL TO USA, XXX) The MOD shall procure through FMS procedures a DOD COMSEC account dedicated to DOD-provided COMSEC equipment and services. As provided by the terms of the LOA establishing the COMSEC account, U.S. personnel will perform central receiving, temporary storage, and transfer services for DOD-provided COMSEC equipment, documents, and keying and other materials; train MOD personnel in the proper custodianship, safeguarding and operation of DOD-provided COMSEC equipment and materials, including keying materials; and conduct periodic inventories and inspections of DOD-provided COMSEC equipment, documents and materials, including keying materials.

(COMMENTS: The general concept is non-negotiable. Details pertaining to periodic inspections, such as dates, notification, etc. can be modified.)

7.2 (U) The MOD shall establish a centralized system in accordance with the current edition of" Allied COMSEC Material Accounting Manual", (NAG-18 series), to distribute and account for DOD-provided COMSEC equipment and material.

(COMMENT: This paragraph is non-negotiable.)

7.3 (X//REL TO USA, XXX) The Parties shall negotiate, agree to, and record the special terms and conditions for each specific DOD/MOD COMSEC equipment, modification, and services project. These terms and conditions shall be documented in FMS LOAs or other appropriate documents, and such LOAs and other documents shall be appended to this MOA in order to provide a record for the Parties of the COMSEC transactions and obligations between them.

ARTICLE VIII

(X//REL TO USA, XXX) DOD-provided COMSEC equipment, keying and other materials, and services shall be for the exclusive use of the MOD. DOD-provided COMSEC equipment, keying and other materials, or the details of DOD-provided support services, shall not be transferred to or revealed in any manner to a third party without the prior written consent of the USG. DOD-provided COMSEC equipment and materials, including keying materials, shall be safeguarded and accounted for in accordance with the procedures prescribed in the current edition of "Safeguarding COMSEC Material

Figure C-B-4. CIS MOA Boilerplate (page 3 of 15)

and Facilities", (NAG-14 series), or other amplifying procedures that may be prescribed by USG authorities. NAG-14 establishes the minimum physical security requirements for the handling and safeguarding of classified COMSEC equipment and material.

(COMMENT: The general concept is non-negotiable. However, approval for third party can be approved and specified here, if there is prior knowledge of the requirement to do so (e.g., MIDS Steering Committee).

ARTICLE IX

(X//REL TO USA, XXX) DOD-provided COMSEC equipment and materials, including keying materials, shall be installed and maintained only by authorized U.S. personnel. This does not preclude, during periods of operational necessity, the one-for-one replacement of malfunctioning equipment by MOD personnel. For purposes of performing required maintenance and periodic inspections, authorized and duly identified U.S. personnel shall be permitted access to DOD-provided COMSEC equipment and material. The MOD shall be notified in advance in those instances when access by authorized U.S. personnel is considered necessary. During periods of such access, U.S. personnel shall be accompanied by appropriately cleared MOD personnel. This does not preclude inspections by MOD, which may be performed at any time.
(COMMENT: This article is non-negotiable.)

ARTICLE X

(U) Only DOD-provided COMSEC keying materials shall be used with DOD-provided COMSEC equipment. Only DOD-provided keying materials shall be used for DOD/MOD bilateral interoperability and for DOD-approved multinational networks involving DOD, MOD, and third parties. DOD-provided COMSEC equipment and materials, including keying materials, shall not be subject to any cooperative development, co-production, co-assembly or production licensing agreements.

(COMMENT: This article is non-negotiable.)

ARTICLE XI

(U) Disagreements or disputes between the Parties arising under or relating to the terms, interpretation, or application of this MOA, or any subsequent modification(s), shall be resolved solely through mutual consultation between the Parties at the lowest feasible level and shall not be referred to any international tribunal or to a third party or persons or entities for resolution or settlement.

(COMMENT: This article is non-negotiable.)

Figure C-B-4. CIS MOA Boilerplate (page 4 of 15)

ARTICLE XII

(U) This MOA may be amended in writing as mutually agreed and executed by authorized representatives of the DOD and the MOD. Such amendments shall be dated, consecutively numbered and appended to each copy of this document.

ARTICLE XIII

(U) Upon completion of the negotiations and/or documentation required pursuant to Paragraph 7.3 of Article VII of this MOA, this MOA shall supersede any temporary loan or other agreements for COMSEC support made previously between individual services of the DOD and of the MOD. Obligations of the Parties concerning security measures, restrictions on use and transfer of equipment, materials including keying materials, or services, and protection of proprietary information shall continue irrespective of termination of this MOA or any previous agreements. LOAs and other implementing transactions shall be terminated in accordance with their terms.

(COMMENT: The last two sentences of this article – beginning with "Obligation of the Parties…." - are non-negotiable.)

ARTICLE XIV

(U) This MOA shall enter into force on the date of the last signature and shall remain in force for 15 years unless earlier terminated upon six months written notice by one Party to the other Party.

(COMMENT: The length of the MOA is negotiable and should always be thoroughly examined.)

For the Department of Defense, United States of America	For the Ministry of Defense, Government of **COUNTRY**
_____ Signature Block	_____ Signature Block
Date:_____	Date:_____

Figure C-B-4. CIS MOA Boilerplate (page 5 of 15)

ANNEX A

CONFIGURATION MANAGEMENT OF TACTICAL COMMAND AND CONTROL

COMMUNICATIONS STANDARDS (U)

GENERAL POLICIES AND PROCEDURES (U)

1. (U) The Parties shall use USG standards to define interoperability parameters. Baseline documents for standards are defined in Appendixes 1 and 2 of this Annex. Provision of technical information or data by the DOD shall be subject to USG releasability requirements.

2. (U) The Parties shall form a technical cooperation group, called the Command and Control Interoperability Board (CCIB). The CCIB shall review proposed tactical C3 systems interoperability change proposals to the defined baseline standards. The Parties shall be equally represented on the CCIB. Meetings shall be held at least annually at a mutually acceptable location. The Parties shall alternate chairmanship of the CCIB.

3. (U) The CCIB shall determine combined interoperability requirements; develop standards and procedures to satisfy interoperability requirements; determine information to be exchanged to support combined C3 interoperability, to include spread spectrum issues and systems; determine appropriate training on approved standards; oversee implementation of approved standards; and ensure the maintenance of approved standards through the application of Configuration Management (CM).

4. (X//REL TO USA, XXX) The Parties shall review any proposed change to the defined procedural standards, as well as to baseline technical standards, prior to adoption of such change. Mutual approval is necessary prior to adoption of any change that may affect interoperability. However, MOD agrees that USG or allie-originated and USG-approved changes to these standards shall be incorporated by MOD if DOD determines the changes are necessary to ensure continued interoperability. This does not preclude MOD from refusing to make system updates at the risk of degrading interoperability.

(COMMENT: This article is non-negotiable.)

Figure C-B-4. CIS MOA Boilerplate (page 6 of 15)

5. (U) A Terms of Reference (TOR) document shall be prepared and agreed to by the CCIB. The TOR will provide specific roles, responsibilities, organizational relationships, methods of work, and taskings of the CCIB in support of this MOA.

6. (U) The CCIB shall plan, coordinate, and evaluate required testing. Test results shall be reviewed by the CCIB along with a test report prepared by the designated test organization. After testing is complete, the CCIB shall recommend appropriate action based on the test results.

(COMMENT: Paragraphs 5 and 6 are only necessary if using paragraphs 2 and 3.)

7. (U) Subject to availability of personnel and resources and subject to signature of appropriate FMS cases, the Parties shall designate office(s) responsible for combined testing; provide systems and personnel necessary to participate in testing in accordance with agreed-to schedules and test plans; fund respective portions of combined testing costs; and implement changes, as required, based on test results.

(COMMENT: This concept is necessary; details may be negotiated.)

8. (U) The CCIB shall: identify the configuration baseline and management documentation that will require maintenance and updates as a result of the CM process; provide procedural, technical, and operational evaluations on all Interface Change Proposals (ICPs); ensure the ICPs are incorporated in appropriate baseline of management documentation; determine the necessity for testing changes and the extent of testing required; recommend approval or disapproval of ICPs to the appropriate MOD and DOD authorities; ensure that agreed ICPs are incorporated in appropriate baseline or management documentation; establish and maintain a configuration status accounting system to track the status of ICPs; and, monitor reports of the use of interoperability standards by operating forces, in order to identify issues requiring corrective action.

(COMMENT: If no CCIB is used, Configuration Baselines need to be identified somewhere within the CIS MOA.)

Figure C-B-4. CIS MOA Boilerplate (page 7 of 15)

9. (U) The Parties shall apply combined CM to defined procedural standards and technical standards. The Parties shall: designate an office responsible for CM; provide qualified personnel to participate in the CCIB, review change proposals, and analyze test results; screen all hardware and software changes to participating systems for possible applicability as changes; submit change proposals as required; provide facilities and test units for interoperability and testing; participate in tests and analyze test results in accordance with test plans, procedures, and schedules to be decided by the CCIB; and provide national positions on changes to those procedures and standards that have multinational interoperability impacts. Data and lessons learned as a result of testing shall be provided to the other Party and action required as a result of testing shall be taken by each Party pursuant to the terms of this MOA.

10. (U) The level of classification of information or data provided in implementation of this MOA shall not be higher than SECRET. The MOD shall ensure that information or data provided under the terms of this MOA shall be safeguarded and afforded protection commensurate with prescribed USG procedures and standards.

11. (U) Information or data shall not be used for the purposes of manufacturing or production of equipment without the prior written consent of the originating Party. Proprietary information or data shall not be used or disclosed in any manner that will prejudice the owner's rights in such information or data. Any plans for production will be addressed under separate agreement.

(COMMENT: This article is non-negotiable.)

12. (U) The originating party shall identify any information or data provided under the terms of this agreement that is subject to limited rights of use. Information or data subject to limited rights of use or disclosure shall not be released to third parties without prior written consent of the originating Party.

(COMMENT: This article is non-negotiable.)

13. (U) Information or data provided under this agreement shall not be disclosed to any other government, individual organization, or third party, including contractors, without the consent of the originating Party.

(COMMENT: This statement must be consistent with Article III.)

Figure C-B-4. CIS MOA Boilerplate (page 8 of 15)

14.. (U) Receipts shall be obtained for all classified information provided; copies of receipts for USG classified information shall be furnished to the sponsoring Service or agency.

(COMMENT: This article is non-negotiable.)

15. (U) Nothing in this MOA diminishes or limits any rights that either Party may have acquired in patents, technical data, or copyrights under any other agreements.

(COMMENT: This article is non-negotiable.)

Figure C-B-4. CIS MOA Boilerplate (page 9 of 15)

ANNEX A, APPENDIX 1

CONFIGURATION DOCUMENTATION (U)

(U) Here is a list of mutually identified and agreed combined configuration items (CIs) for procedural interface standards that are subject to configuration management within the Command and Control Interoperability Board (CCIB). Applicable CI baseline documentation is included for each CI.

Procedural Interface	Baseline Documents
TDL A and B	MIL-STD 6011
TDL J	MIL-STD 6016
U.S. Message Text Formats	MIL-STD 6040
Variable Message Format (VMF)	MIL-STD 6017
Data Forwarding Between Tactical Data Links	MIL-STD 6020
Standard Symbology	MIL_STD 2525
Joint Range Extension Application Protocol (JREAP)	MIL_STD 3011
Joint Multi-Tactical Data Link Operating Procedures (JMTOP)	CJCSM 6120.01D

(COMMENT: All Applicable CI's and MIL-STDs will be provided to all Partner Nations upon successful completion of U.S. foreign disclosure staffing which includes COCOM validation of the applicable requirement that justifies the release.)

Figure C-B-4. CIS MOA Boilerplate (page 10 of 15)

ANNEX A, APPENDIX 2

DEFINITIONS (U)

1. (U) Baseline Documentation. Document(s) formally designated and fixed at a specific time during the life cycle of a configuration item. The document constitutes a baseline where changes must first be approved through an established CM process. Applicable documents include but are not limited to:

a. (U) Tactical Command and Control Communications and Procedural Standards. Documents that contain operational message standards, or procedures, to achieve compatibility and interoperability between tactical command and control systems. All releasable changes to these standards will be provided to the MOD.

b. (U) Combined Interface Operating Procedures (CIOP). Provides system compatibility information and detailed functional descriptions and procedures used by operators for establishing and maintaining a procedural standards interface. These procedures will be developed by the CCIB.

c. (U) Applicable Spread Spectrum Technical Standards. Baseline documents will be identified as an update when MOD requests are forwarded to DOD for foreign release approval.

2. (U) Bit-Oriented Messages (BOMs). Messages that are structured in binary digits, restricting them to machine interpretation since composition and readability by humans requires translation aids. M-Series messages and V/R-Series messages used in TDLs A, B, and J are examples of BOMs.

3. (U) Change Proposals

a. (U) A change proposal recommends a change to the baseline documentation of a standard (e.g., a data link, or data link system implementation of a Technical Interface Specification). Change proposals will be processed according to the procedures agreed upon in the TOR document for the CCIB. The Configuration Management Plan will define the change proposal format requirements and submission process.

Figure C-B-4. CIS MOA Boilerplate (page 11 of 15)

b. (U) Interface Change Proposal (ICP). ICP is a change to the procedural standards to maintain interoperability, or a change to the operational procedures that are used to establish and maintain an interface. An ICP is a document used to introduce a change to procedural interface standards documents and management documents that are placed under CM. As a minimum, an ICP will contain an analysis of impact from the perspective of the submitting nation.

4. (U) Configuration Management (CM). A discipline applying technical and administrative direction and oversight to identify and document the functional and physical characteristics of configuration items (CIs); audit the CIs to verify conformance to specifications, interface control documents, and other contract requirements; control changes to CIs and their related documentation; and record and report information needed to manage CIs effectively.

5. (U) Message Text Format (MTF). A specified sequence of main text set formats having a unique message text format identifier. Formatted messages can be used for voice or record traffic purposes and are intended to be both man and machine readable. MTFs implemented for U.S. use are called USMTFs and are documented in MIL-STD 6040.

6. (U) Procedural Interface Standard. Specifications for the manner of accomplishing the exchange of information across an interface. It defines: (a) the form or format in which information is to be exchanged; (b) the prescribed information exchange language, syntax, and vocabulary to be used in the information exchange; and (c) interface operating procedures that govern the information exchange.

7. (U) Tactical Digital Link (TDL). A U.S. Joint Staff-approved standardized communications link suitable for transmission of digital information via BOMs, i.e., a joint data link. A TDL is characterized by standardized message formats and transmission characteristics. Additional TDL information can be found in CJCSI 6610.01C (reference y).

a. (U) TDL A. A half-duplex secure netted digital data link utilizing parallel transmission frame characteristics and standard message formats at either 1364 or 2250 bits per second.

b. (U) TDL B. A full-duplex secure point-to-point data link utilizing serial transmission frame characteristics and standard message formats at 5000 bits per second.

Figure C-B-4. CIS MOA Boilerplate (page 12 of 15)

c. (U) TDL J. A secure, high capacity, jam resistant, nodeless data link which uses the Joint Tactical Distribution System (JTIDS) or Multifunctional Information Distribution System (MIDS) transmission characteristics and the protocols, conventions, and fixed-length message formats defined by the JTIDS Technical Interface Design Plan (TIDP).

8. (U) Technical Interface Specification (TIS). A document intended primarily for use in defining technical interface characteristics of C3 systems or equipment employed in joint or combined tactical operations. Establishes the baseline documentation for configuration management of C3I systems and equipment interoperability. Describes essential technical requirements that must be met to provide interoperability. Establishes design parameters that will ensure interoperability requirements in tactical C3 employments.

9. (U) Technical Interface Standards. Specifications of the functional, electrical, and physical characteristics necessary to allow the exchange of information across an interface between different tactical C3 systems or equipment.

10. (U) Testing. Testing during the life cycle of the interface standards assures that interoperability is maintained. Two types of testing are normally required:

a. (U) Operational Maintenance Testing. Tests conducted to ensure that MOD systems implementing the procedural and technical standards are interoperable with U.S. systems. These tests will evaluate the degree of interoperability that has been achieved through the implementation of the standard by participating C3 systems.

b. (U) Requalification Testing. Tests conducted to ensure that systems remain compatible and interoperable following system software changes or additions directly associated with the implementation of these procedural and technical standards.

Figure C-B-4. CIS MOA Boilerplate (page 13 of 15)

ANNEX B

PROVISION OF COMMUNICATIONS SECURITY
EQUIPMENT AND SERVICES (U)

(COMMENT: If this information is already covered in the body of the CIS MOA, this annex may be eliminated.)

RESPONSIBILITIES OF THE PARTIES (U)

1. (U) The U.S. Department of Defense (DOD) shall:

a. (X//REL TO USA, **XXX**) Provide releasable and approved DOD COMSEC equipment, keying and other materials, and services to the MOD in accordance with Article VI of this MOA in order to satisfy mutually identified U.S./**COUNTRY** Armed Forces requirements for secure communications interoperability.

b. (X//REL TO USA, **XXX**) Support the MOD COMSEC account in accordance with the terms of the relevant LOA that MOD shall establish in accordance with Article VII of this MOA. Such support shall include: (i) providing MOD personnel with training regarding procedures required to operate, safeguard, and account for DOD-provided COMSEC equipment and material in accordance with Article VII of this MOA; (ii) providing or arranging for the installation and maintenance of DOD-provided COMSEC equipment in accordance with Article IX of this MOA, and; (iii) inspecting DOD-provided COMSEC equipment and materials periodically to ensure that they are being handled, used, and safeguarded in accordance with prescribed DOD procedures and standards in accordance with Article VII of this MOA.

2. (U) The **COUNTRY** Ministry of Defense (MOD) shall:

a. (U) Ensure that DOD-provided COMSEC equipment and materials including keying materials are safeguarded and afforded protection commensurate with prescribed DOD procedures and standards in accordance with Articles VII through X of this MOA.

b. (U) Provide the funding required to establish, operate, and sustain a DOD COMSEC account dedicated to the equipment and services provided by the DOD to the MOD in accordance with Article VII of this MOA.

c. (U) Send personnel to DOD training on procedures to operate, safeguard, and account for DOD-provided COMSEC equipment and materials including keying materials under the terms of the LOA described in Article VII of this MOA.

Figure C-B-4. CIS MOA Boilerplate (page 14 of 15)

d. (U) Establish a centralized system to distribute and account for DOD-provided COMSEC equipment and materials including keying materials in accordance with Article VII of this MOA.

e. (X/REL TO USA/**XXX**) In accordance with Article VIII of this MOA, ensure that DOD-provided COMSEC equipment and materials including keying materials are used only for mutually identified U.S./**COUNTRY** Armed Forces secure interoperability requirements, and that such equipment and materials are not revealed in any manner to or transferred to a third party.

f. (U) In accordance with Article X of this MOA, ensure that only keying materials provided by the DOD are used with DOD-provided COMSEC equipment.

g. (U) In accordance with Article IX of this MOA, arrange for access by authorized and duly identified U.S. personnel to DOD-provided COMSEC equipment and materials including keying materials for necessary maintenance and periodic inspections.

h. (U) Ensure that safeguard procedures established in accordance with Article VIII of this MOA include requirements that emergency destruction procedures are implemented whenever loss or compromise of DOD-provided COMSEC equipment or material appears imminent and that DOD authorities are notified as expeditiously as possible of any loss or suspected compromise of DOD-provided COMSEC equipment or material.

3. (X/REL TO USA/**XXX**) In accordance with Article VII of this MOA, the Parties shall negotiate, agree to, and record the special terms and conditions for each specific DOD/MOD COMSEC equipment, modification and services projects.

Figure C-B-4. CIS MOA Boilerplate (page 15 of 15)

APPENDIX C TO ENCLOSURE C

PROCEDURES AND BOILERPLATE FOR AN INFOSEC EQUIPMENT AGREEMENT

1. General. The INFOSEC equipment agreement (IEA) is an international agreement between the U.S. Department of Defense (DOD) and a foreign government MOD (or equivalent). An IEA provides the legal framework for the short-term and/or isolated loan and safeguard of COMSEC products and information to support a specific interoperability requirement. "Loan," in this context, refers to the transfer to the foreign nation of released COMSEC products that the combatant command has purchased; it does not imply any form of sale, FMS-CDS transaction, or long-term transfer. An IEA does not provide for the establishment of a CCIB or a foreign MOD funded COMSEC accounting mechanism. Under an existing IEA, if more approved devices under a particular interoperability requirement are necessary, then the existing IEA must be amended with an annex listing the additional equipment. If a new interoperability requirement is needed, then a new IEA must be negotiated and a new CRR submitted to the Joint Staff and the DIRNSA.

2. Authority to Negotiate and Conclude. Within the Department of Defense, the authority to negotiate and conclude IAs originates with the Secretary of Defense. DODD 5530.3 (reference f), CJCSI 2300.01D (reference l) and CJCSI 6740.01B (reference m) delegate the authority in separate areas of cognizance to the Secretaries of the Military Departments, certain Under or Assistant Secretaries of Defense, the Chairman of the Joint Chiefs of Staff, and Directors of Defense agencies. DIRNSA has been delegated the authority to negotiate and conclude international COMSEC products and services agreements. Further delegation to the combatant commands to negotiate and conclude international COMSEC product and services agreements is authorized.

3. COMSEC Accounting Mechanisms. The combatant command and its supporting Headquarters/Component COMSEC Material Control System (CMCS) infrastructure will be responsible for maintaining accountability of COMSEC material or products released under an IEA. The combatant command's supporting U.S. COMSEC account will issue, account for, and control released COMSEC products in accordance with guidelines established by its COR. The combatant command may also negotiate with other USG departments/agencies to provide accountability for COMSEC products transferred under an IEA.

4. IEA Preparation/Conclusion Procedures. The following paragraphs describe the steps in preparing, negotiating, and concluding an IEA.

a. Step One -- Combatant Command Interoperability Requirement. Combatant command identifies a combined interoperability requirement that requires the release of U.S. COMSEC product(s) to a foreign government. The combatant command sends the CRR to the Joint Staff for validation in accordance with the procedures in Enclosure C. If the combatant command proposes to support the release with an IEA, it initiates this process in tandem with submission of a CRR.

b. Step Two -- Utilize Current IEA Boilerplate. The combatant command should replace all references in the boilerplate document (Figure C-C-1, below) to reflect the specific foreign nation and MOD with who the agreement will be. The combatant command should also appropriately classify the agreement. The language in the boilerplate IEA has been approved by DIRNSA and reflects the minimum responsibilities to be included in COMSEC agreements with foreign nations. The template in the Annex to this appendix shall serve as the baseline document. Any substantive deviations from this boilerplate document must be approved by the Joint Staff and the DIRNSA.

c. Step Three -- Prepare IEA and Internally Coordinate Request for Authority to Negotiate and Conclude IEA Package. Combatant command prepares a memorandum to the DIRNSA requesting authority to negotiate and conclude an IEA. Combatant command staff coordinates command memorandum and draft IEA. After coordination is concluded, combatant command commander signs the memorandum and forwards to the DIRNSA.

d. Step Four -- Submit IEA Package to the DIRNSA for Approval. Combatant command sends the draft IEA to the DIRNSA.

e. Step Five -- DIRNSA Reviews IEA and Delegates to Combatant Command Authority to Negotiate and Conclude. The DIRNSA reviews the draft IEA and, if there are no substantive changes, notifies the combatant command of authorization to negotiate and conclude the IEA.

f. Step Six -- Combatant Command Negotiates and Concludes IEA. After receiving the DIRNSA delegation authority, the combatant command may provide the foreign government with a copy of the draft IEA before negotiations. Generally, the combatant command provides the IEA to the DATT or SAO at the American embassy, and the DATT or SAO provides a copy to the foreign government MOD. The combatant command tailors a negotiation team with representation from NSA as required. During negotiations, the combatant

command should explain the foreign users' responsibilities under the IEA to safeguard the COMSEC products and information. If the foreign MOD proposes no substantive changes to the draft text, the combatant command may conclude the IEA. After the IEA is signed, the combatant command will forward reproducible copies of the IEA to General Counselof the Department of Defense (Washington, D.C. 20301-1600), NSA Information Assurance Operations Group (DP2), and the Joint Staff. Finally, the combatant command will keep a copy of all signed and concluded IEAs for an official record.

g. Step Seven -- Combatant Command Transfers COMSEC Products/Information. Once the foreign MOD signs the IEA, the combatant command may transfer U.S. COMSEC products and information to the foreign nation. The combatant command's supporting U.S. COMSEC account will issue, account for, and control released COMSEC products in accordance with guidelines established by its COR.

INFOSEC EQUIPMENT AGREEMENT BOILERPLATE

(CLASSIFICATION)

EQUIPMENT AGREEMENT

BETWEEN

UNITED STATES GOVERNMENT

AND

XXX COUNTRY NAME
XXX COUNTRY GOVERNMENT NAME (IF KNOWN)
XXX COUNTRY INFORMATION ASSURANCE ORGANIZATION (IF KNOWN)

PERTAINING TO THE PROVISION OF ***ZZZ EQUIPMENT***

Date Signed:_____

Derived From:	Classification Guide for Information Systems Security
Dated:	March 1992
Declassify On:	Source Marked "OADR"
Date of Source:	March 1992

Figure C-C-1. INFOSEC Equipment Agreement Boilerplate (page 1 of 6)

1. (U) PURPOSE AND SCOPE

(X//REL TO USA, XXX) In order to assist in the establishment of secure voice communications between the United States Government (USG) and the ***XXX COUNTRY NAME***, USG will make available ***ZZZ EQUIPMENT*** to ***XXX***, consistent with section 421 of title 10 of the United States Code (10 USC 421), NSTISSP No. 8, and other relevant laws, regulations, and policy guidance. This document defines the scope, conditions, and responsibilities of the USG and ***XXX*** pertaining to ***ZZZ*** equipment. This equipment agreement is not intended, and shall not be construed to be an "international agreement" within the meaning of section 112b of title 1 of the United States Code 91 USC 112b).

2. (U) DEFINITIONS

a. (U//FOUO) Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived telecommunications and to ensure the authenticity of much telecommunications. Communications security includes crypto security, transmissions security, emissions security, and physical security of COMSEC materials.

b. (U//FOUO) Make Available. The provisions of the ***ZZZ*** by the USG under specified conditions, such that USG retains ownership of and title to the equipment (to include the units themselves and any ancillaries, plus associated COMSEC material and operating manuals provided by USG).

c. (U//FOUO) Controlled Cryptographic Item (CCI). Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements.

3. (U) GENERAL PROVISIONS

(U//FOUO) All activities of the Parties under this agreement shall be carried out in accordance with their national laws. Any costs for support of financial obligations under this agreement are subject to enabling national legislation and the availability of funds appropriated for such purposes. References to provisions of U.S. law, to include references to specific U.S. regulations or policy guidance shall be construed to include future versions of such provisions of law, regulations, or policy guidance unless otherwise stated herein.

Figure C-C-1. INFOSEC Equipment Agreement Boilerplate (page 2 of 6)

4. (U) AGREEMENTS

a. *(X//REL TO USA, XXX)* The USG will make available ***ZZZ*** secure communications equipment to ***XXX*** in accordance with the provisions of paragraph 5 below to satisfy mutually identified secure interoperability requirements between the USG and ***XXX***.

b. *(X//REL TO USA, XXX)* The title of the USG furnished ***ZZZ*** equipment shall remain at all times with USG. The receiving party (***XXX***) shall not transfer possession or permit use of the equipment or the services to another party without the express written authorization of the USG. In that regard, the ***ZZZ*** equipment made available to ***XXX*** is for its exclusive use and only for its secure communications with USG and other USG authorized parties. Details concerning ***ZZZ*** equipment and services provided by USG shall not be revealed in any manner to, or released to, any third country or representative without prior written consent of the USG.

c. (U//FOUO) The ***ZZZ*** equipment made available to ***XXX*** is to be CCI. The equipment and associated material are very sensitive and require safeguarding in accordance with the NAG-14C, SAFEGUARDING COMSEC MATERIAL AND FACILITIES, dated December 1997 and NAG-18A, ALLIED COMSEC MATERIAL ACCOUNTING MANUAL, dated July 1990.

d. (U//FOUO) Only COMSEC keying material provided by the USG will be used with the ***ZZZ*** equipment provided under this agreement.

e. (U//FOUO) The ***ZZZ*** equipment will not be subject to any cooperative development, co-production, co-assembly or production licensing agreements.

f. (U//FOUO) The Parties acknowledge and agree that their performance under this agreement does not violate their national laws, regulations, or policies, nor is this agreement to be implemented or interpreted to require any acts or commitments which are in violation of their national laws, regulations, or policies.

5. (U) RESPONSIBILITIES

a. (U) The USG shall:

(1) *(X//REL TO USA, XXX)* Make available the ***ZZZ*** equipment, associated keying material and supporting technical documentation material in quantities mutually agreed to by the respective parties in order to achieve secure communications interoperability as described in Section 1, above.

(2) (U//FOUO) Provide initial training regarding procedures which are required to safeguard, control, and manage the USG equipment and keying material.

Figure C-C-1. INFOSEC Equipment Agreement Boilerplate (page 3 of 6)

(3) (U//FOUO) Provide initial training regarding the proper methods for operating the ***ZZZ*** equipment.

(4) (U//FOUO) Arrange for the maintenance of the ***ZZZ*** equipment.

(5) (U//FOUO) Confirm, every six months through mutually agreed procedures, that the ***ZZZ*** equipment and keying material are handled, used, safeguarded, controlled, and managed in accordance with prescribed procedures and standards mutually agreed to by both governments.

b. (U) ***XXX*** shall:

(1) (U//FOUO) Ensure the USG ***ZZZ*** equipment and keying material is safeguarded and afforded protection commensurate with NAG-14C and NAG-18A.

(2) (U//FOUO) Ensure USG provided ***ZZZ*** equipment and material is used only for ***USG approved*** secure interoperability requirements.

(3) (U//FOUO) Ensure USG-provided ***ZZZ*** equipment and material is not reallocated to any other nation(s) or nongovernmental organization(s).

(4) (U//FOUO) Ensure that only USG supplied keying material is used.

(5) (U//FOUO) Arrange for access by authorized and duly identified USG personnel to the ***ZZZ*** equipment and material for necessary maintenance, inspections, and inventories to maintain USG accountability.

(6) (U//FOUO) Ensure that emergency key zeroization procedures are implemented in those instances where the loss, capture, or compromise of the ***ZZZ*** equipment or material appears imminent.

(7) (U//FOUO) Notify the USG as soon as possible and no later than 72 hours of any loss or suspected compromise of USG provided ***ZZZ*** equipment or keying material.

6. (U) ACCOUNTABILITY AND CONTROL OF EXCHANGED INFORMATION

a. (U//FOUO) USG ***ZZZ*** equipment and keying material provided under the terms of this agreement will be safeguarded, controlled and managed in accordance with NAG-14C and NAG-18A. The aforementioned doctrine establishes the minimum physical security requirements for the handling and safeguarding of ***ZZZ*** equipment and keying material.

Figure C-C-1. INFOSEC Equipment Agreement Boilerplate (page 4 of 6)

b. (U//FOUO) It is understood that loss caused by war or natural disasters may be unavoidable. If a particular loss under such circumstances is mutually agreed to have been unavoidable, ***XXX***, after discussions with USG, may be relieved of accountability and liability.

7. (U) MAINTENANCE

(U//FOUO) The USG shall arrange all required maintenance on the ***ZZZ*** equipment. The point of contact for reporting problems is the combatant command J-6.

8. (U) DISPUTES

(U//FOUO) All disagreements or disputes between Parties arising under or relating to the terms, interpretation, or application of this agreement, or any subsequent modification(s), shall be resolved only by consultation between Parties at the lowest feasible level and shall not be referred to an individual, a third party, an international tribunal, or any other forum of resolution or settlement.

9. (U) LANGUAGE

(U//FOUO) This agreement, along with any subsequent agreement, is executed in the English language only.

10. (U) DURATION

a. (U//FOUO) This agreement and the provision of ***ZZZ*** equipment to ***XXX*** may be terminated by either of the Parties through written notification or, alternatively, by ***XXX*** through the acknowledged return and acceptance of the ***ZZZ*** equipment to the USG.

b. (U//FOUO) To help ensure interoperability and other considerations regarding functionality, the USG will make the ***ZZZ*** equipment available for a period of up to five years. If the Parties to this agreement determine that the need for the ***ZZZ*** equipment will continue after the end of 5 years from the effective date of this agreement, the USG shall take appropriate action to negotiate a new agreement consistent with U.S. law at that time.

c. (U//FOUO) Upon termination of the ***ZZZ*** equipment agreement with ***XXX***, all equipment and keying material shall be returned immediately to the USG.

11. (U) REVIEW

(U//FOUO) The terms and conditions of this agreement shall be reviewed upon request by either of the Parties.

Figure C-C-1. INFOSEC Equipment Agreement Boilerplate (page 5 of 6)

12. (U) AMENDMENTS

(U//FOUO) Amendments to this agreement will be in writing, mutually agreed to by the Parties, and executed by authorized representatives of the USG and ***XXX***. A copy of all amendments will be appended to each copy of this document, dated, and consecutively numbered.

13. (U) ANNEXES

(U//FOUO) Annexes may be appended and agreed to, as necessary, to implement provisions of this agreement.

14. (U) VALIDATION

(U//FOUO) This agreement shall enter into force on the date it is signed by the authorized representatives of the USG and ***XXX***.

_____	_____
NAME	
NAME	
Title	
Title	
_____	_____
Date of Signature	Date of Signature

Figure C-C-1. INFOSEC Equipment Agreement Boilerplate (page 6 of 6)

(INTENTIONALLY BLANK)

ENCLOSURE D

REFERENCES

a. DOD Instruction 8523.01, 22 April 2008, "Communications Security (COMSEC)"

b. (FOUO) National Security Telecommunications Information Systems Security Policy (NSTISSP) No. 8, 13 February 1997, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated COMSEC Information to Foreign Governments (FOUO)"

c. Committee on National Security Systems Directive (CNSSD) No. 502, 16 December 2004, "National Directive on Security of National Security Systems"

d. National Disclosure Policy (NDP) 1, 1 December 1998, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations"

e. Department of Defense Directive (DODD) 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

f. DOD Directive 5530.3, 11 June 1987, as amended, "International Agreements"

g. SECAN Doctrine and Information Publication (SDIP) 293, May 2007, "Instructions for the Control and Safeguarding of NATO Cryptomaterial"

h. AC/35-D/2004-Rev1, 19 October 2006, "NATO Security Committee Primary Directive on INFOSEC"

i. MC 74/3 Corrigendum 3, 23 April 2004, "Communications Security for NATO"

j. Document C-M (2002) 49, 17 June 2002, "Security Within the North Atlantic Treaty Organization (NATO)"

k. National Security Directive (NSD) No. 42, 5 July 1990, "National Policy for the Security of National Security Telecommunications and Information Systems"

l. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 2300.01 series, "International Agreements"

m. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6740.01 series, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations"

n. Executive Order 11958, 18 January 1977, as amended, "Administration of Arms Export Controls"

o. National COMSEC Instruction (NACSI) No. 6001, 21 December 1984, "Foreign Military Sale of Communications Security Articles and Services to Foreign Governments and International Organizations"

p. OASD (NII) Department of Defense Global Positioning System (GPS) Security Policy, 4 April 2006

q. Title 10, United States Code, "Armed Forces"

r. National Security Agency/Central Security Service (NSA/CSS) Policy Manual No. 3-16, 05 August 2005, "Control of Communications Security (COMSEC) Material"

s. National Security Telecommunications Information Systems Security Instruction (NSTISSI) No. 4005, August 1997, "Safeguarding Communications Security (COMSEC) Facilities and Materials"

t. Non-crytpographic Operational General (NAG) 14C, December 1997, "Safeguarding COMSEC Material and Facilities"

u. Non-crytpographic Operational General (NAG) 18A, July 1990, "Allied COMSEC Material Accounting Manual"

v. Department of Defense Directive (DODD) 5100.20, 26 January 2010, "National Security Agency/Central Security Service (NSA/CSS)"

w. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 2700.01 series, "International Military Agreements for Rationalization, Standardization, and Interoperability Between the United States, Its Allies, and Other Friendly Nations"

x. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6010.01 series, "Coordination of United States Command, Control, Communications, and Computer Systems Positions in International Forums"

y. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6610.01 series, "Tactical Data Link Standardization Implementation Plan"

z. National Security Telecommunications Information Systems Security Instruction (NSTISSI) No. 4002, 5 June 1986 (as amended 16 March 2010), "Classification Guide for COMSEC Information"

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A

AOR	Area of Responsibility
ASD NII	Assistant Secretary of Defense (Networks and Information Integration)
ATM	asynchronous transfer mode

C

C3	command, control and communications
C3I	command, control, communications, and intelligence
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, and intelligence, surveillance, and reconnaissance
CCEB	Combined Communications-Electronics Board
CCIB	Command and Control Interoperability Board
CCI	controlled cryptographic items
CDS	cryptographic device services
CI	configuration item
CIOP	combined interface operating procedures
CIP	Combined Interoperability Program
CIR	COMSEC interoperability requirement
CIS MOA	Communication Interoperability and Security Memorandum of Agreement
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CM	configuration management
CMCS	COMSEC Material Control System
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COCOM	combatant command (legal authority)
COMSEC	communications security

COR	central office of record
CRR	COMSEC Release Request
CSS	Central Security Service

D

DATT	Defense Attaché
DCS	Direct Commercial Sales
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DJS	Director, Joint Staff
DOD	Department of Defense
DODD	Department of Defense Directive
DSCA	Defense Security Cooperation Agency

E

ENDP	Exception to the National Disclosure Policy

F

FMS	foreign military sales

G

GC	General Counsel
GPS	global positioning system

H

HAE	host application environment
HOD	Head of Delegation

I

IA	international agreement
IAW	in accordance with
ICP	interface change proposal
IEA	INFOSEC equipment agreement
IFF	identification, friend or foe
INFO	information addressee on message
INFOSEC	information systems security
IP	Internet protocol
IPO	International Program Office
ISR	intelligence, surveillance, and reconnaissance

J

JMTOP	Joint Multi-tactical Data Link Operating Procedure
JREAP	Joint Range Extension Application Protocol
JTIDS	Joint Tactical Information Distribution System

K

KEYMAT	key material

L

LOA	Letter of Offer and Acceptance
LOR	Letter of Request

M

MIDS	multifunction information display system
MIL-STD	military standards
MOA	memorandum of agreement
MOD	Ministry of Defense
MOU	memorandum of understanding
MTF	message text format

N

NACSI	National COMSEC Instruction
NAG	Non-cryptographic Operational General Document
NATO	North Atlantic Treaty Organization
NDP	National Disclosure Policy
NSA	National Security Agency
NSD	National Security Directive
NSTISSI	National Security Telecommunications Information Systems Security Instruction
NSTISSP	National Security Telecommunications Information Systems Security Policy

O

OADR	originating agency's determination required

P

PMO	program management office
POC	point of contact
PPS	precise positioning system

R

RIP	release in principle
RIS	release in specific
REL	releasable

S

SAASM	Selective Availability and Anti-Spoofing Module
SAO	Security Assistance Office
SATCOM	Satellite Communications
SDIP	SECAN Doctrine and Information Publication
SDR	software defined radio
SECAN	Military Committee Communications Security and Evaluation Agency
SINCGARS	Single Channel Ground to Air Radio System
SIGINT	signals intelligence
SIPRNET	Secret Internet Protocol Router Network
SRR	Ship Rider Request

T

TA/CP	technology assessment/control plan
TCP	Theater Campaign Plan
TDL	tactical data link
TET	temporary equipment transfer
TIDP	technical interface design plan
TIS	technical interface specification
TOR	terms of reference

U

USCENTCOM	Central Command
USDELMC	United States Military Delegation to NATO
USG	United States government
USMTF	United States message text format

V

VMF	variable message text format

PART II – DEFINITIONS

Associated COMSEC Information. COMSEC techniques and services used to provide confidentiality, authentication, integrity, non-repudiation, and reliable delivery of information contained in national security systems, or to protect national security information. It includes, but is not limited to, cryptographic algorithms, technology, keying material, as well as cryptologic systems and techniques implemented in hardware, software, or firmware.

Classified National Security Information. Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmissions security, emissions security, and physical security of COMSEC materials.

COMSEC Product. Item (chip, module, assembly, or equipment), technique, or service that performs or relates to information systems security.

Direct Commercial Sales. Non-government contracts between U.S. industry and a foreign purchaser. For U.S. COMSEC products, only applies to NATO and CCEB nation purchases.

Endorsement. An official acknowledgment and/or approval for support by a combatant command of a U.S. Government (USG), DOD, or applicable international organization requirement or activity in their AOR where the release of U.S. COMSEC products or information to a foreign partner or international organization is required.

Information Systems Security (INFOSEC). Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

National Disclosure Policy (NDP-1). National policy and procedures in the form of specific disclosure criteria and limitations required by U.S. departments and agencies having occasion to release classified U.S. military information to foreign governments and international organizations. NDP-1 provides for the management of an interagency mechanism and procedures required for the effective implementation of the policy.

National Security Systems. Any telecommunications or information system operated by the USG, the function, operation, or use of which:

(1) Involves intelligence activities;
(2) Involves cryptologic activities related to national security;
(3) Involves the command and control of military forces;
(4) Involves products that are an integral part of a weapon or weapons system;
(5) Is critical to the direct fulfillment of military or intelligence missions, but not including routine administrative and business information such as payroll, finance, logistics, and personnel management information.

Release. A deliberative review and decision process undertaken by the CNSS and National Manager to share, either on a temporary or permanent basis, U.S. COMSEC products or associated COMSEC information with foreign governments or international organizations in satisfaction of USG foreign policy and military or economic objectives.

Release in Principle (RIP). A RIP provides a USG policy decision to share COMSEC information, products, or services in support of a secure interoperability requirement. A RIP is not an approval to physically transfer a COMSEC product. With an approved RIP, combatant commands, U.S. Military Services and their components, and DOD departments and agencies can *discuss* COMSEC products or associated COMSEC information requirements and develop *proposed* solutions with foreign nations to fulfill U.S. secure interoperability requirements. The combatant command must submit a second COMSEC release request (CRR) for specific products to the CJCS for validation. The second CRR will result in a release in specific and is described in the next paragraph.

Release in Specific (RIS). A RIS provides a USG policy decision to share a defined set (quantity and nomenclature) of COMSEC information, products, or services with specified foreign governments. RISs do not authorize equipment transfer, per se. However, because RISs are specific by definition, they usually provide the national manager the required information to approve transfer concurrent to and in accordance with RIS approval.

Ship Rider. Ship rider procedures are a DIRNSA approved procedure used to solve short-term interoperability requirements. The procedure requires U.S. cleared personnel to temporarily install, operate, key, and physically secure U.S. COMSEC products in a foreign government weapon or C4I system in foreign sites or mobile platforms.

Temporary Equipment Transfer (TET). Temporary relocation of a released COMSEC product necessary to support the interoperability requirement for which the product was released. The combatant command shall approve TET requests. The DIRNSA shall approve permanent relocations, subject to combatant command endorsement.

Transfer. To provide, by means of sale, lease, loan, or other means, COMSEC products or associated COMSEC information to a foreign government or international organization.

(INTENTIONALLY BLANK)