DEFENSE SECURITY COOPERATION AGENCY
2800 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2800

11 JAN 2020

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF THE AIR FORCE FOR INTERNATIONAL AFFAIRS
DEPUTY ASSISTANT SECRETARY OF THE ARMY FOR DEFENSE EXPORTS AND COOPERATION
DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR INTERNATIONAL PROGRAMS
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
DIRECTOR FOR SECURITY ASSISTANCE, DEFENSE FINANCE AND ACCOUNTING SERVICE - INDIANAPOLIS OPERATIONS
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE LOGISTICS INFORMATION SERVICE
DIRECTOR, DEFENSE LOGISTICS AGENCY DISPOSITION SERVICES
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, NATIONAL GEOSPATIAL - INTELLIGENCE AGENCY
DEPUTY DIRECTOR FOR INFORMATION ASSURANCE, NATIONAL SECURITY AGENCY

SUBJECT: Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) and Communications Security (COMSEC) Policy Update, Defense Security Cooperation Agency (DSCA) Policy 20-74 [SAMM E-508]

This memorandum rescinds DSCA Policy 18-52, 13-12, and 09-36 and updates the relevant chapters of the SAMM as detailed in the attachment to clarify and further define policy pertaining to Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) and Communications Security release, transfer, and transportation. These changes are effective immediately and will be included in the online version of the SAMM at http://samm.dsca.mil. Implementing Agencies should disseminate this policy to supporting activities.

Summary of changes:

- Further defines C4ISR release and transfer policy
- Eliminates requirement for NSA Authorization to Sell memoranda for specific COMSEC products to specified countries
- Clarifies COMSEC release requirements for Congressional Notifications
- Clarifies COMSEC requirements for Price and Availability and Letters of Offer and Acceptance

- Establishes Network Enabled Weapons COMSEC release and Enhanced End-Use Monitoring requirements
- Establishes COMSEC/Controlled Cryptographic Item (CCI)-unique Transportation Plan
- Establishes release requirements for Cross Domain Solutions
- Clarifies COMSEC/CCI transportation policies to authorizes shipment of CCI by Freight Forwarders to all authorized purchasing nations

If you have any questions concerning this guidance, please contact DSCA-DSA/WPNS, International C4I Programs Mr. Chris King, christopher.s.king26.civ@mail.mil, (703) 697-9963 or Mr. Rob Sprout, robert.h.sprout.civ@mail.mil, (703) 697-9817. For questions relating to the SAMM, Security Assistance Management Manual, please contact DSCA-STR/SPI, Ms. Melissa Dockstader, Strategic Planning and Integration Division, at (703) 692-6657 or e-mail: melissa.m.dockstader.civ@mail.mil.

Cara L. Abercrombie
Acting Deputy Director

cc:
STATE/PM-RSAT
AFRICOM
CENTCOM
EUCOM
INDOPACOM
NORTHCOM
SOCOM
SOUTHCOM
TRANSCOM
USACE
USASAC
USASAC-NC
SATFA
TRADOC
NAVSUP WSS
NAVICP
NETSAFA
AFSAC
AFSAT
DSCU
MARCORIP
SCETC
USCG International Affairs (G-CI)

SAMM E-Change 508

Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) and Communications Security (COMSEC) Policy Update

1) **Replace C3.7.3. in its entirety (except C3.T6) with the following:**

C3.7.3. Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR).

C3.7.3.1. C4ISR Definitions.

C3.7.3.1.1. C4ISR. C4ISR encompasses systems, procedures, and techniques used to collect and disseminate information. It includes intelligence collection and dissemination networks, command and control networks, and systems that provide the common operational/ tactical picture. It also includes information assurance products and services, as well as communications standards that support the secure exchange of information by C4ISR systems. Under the C4ISR umbrella, operators use systems to exchange digital, voice, and video data with appropriate levels of command. The two key aspects of C4ISR systems are access to secure networks controlled by Information Security (INFOSEC) products and services, and classified data processed on C4ISR networks. See CJCSI 6510.06 series (not for public release) for information on the release of U.S. INFOSEC products (Communications Security (COMSEC), cryptographic algorithms, cryptographic key material, security infrastructure) to foreign purchasers.

C3.7.3.1.2. INFOSEC. INFOSEC is the 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 threat. INFOSEC is applied through the application of Cybersecurity and COMSEC.

C3.7.3.1.3. COMSEC. COMSEC is the measures and controls taken to deny unauthorized persons' information derived from telecommunications and other information systems, and technologies necessary to ensure the authenticity of such communications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. Secure telecommunication or information system cryptographic components are the primary COMSEC products for transmission security and commonly called COMSEC devices or products. COMSEC devices are designated Controlled Cryptographic Items (CCI).

C3.7.3.1.4. Controlled Cryptographic Item (CCI). CCIs are devices approved by the National Security Agency that embody cryptographic logic or other cryptographic design, but do not perform the entire COMSEC function. CCIs are dependent upon host equipment or assemblies to complete and operate COMSEC functions. Un-keyed CCI is unclassified. An item may be designated CCI because its entire component is controlled (e.g. Inline Network Encryptor (INE)), or because the item contains an embedded cryptographic NSA Type-1 certified module to encrypt/de-encrypt information (e.g. secure radio).

C3.7.3.2. C4ISR Responsibilities. Table C3.T6. lists organizations and their C4ISR responsibilities.

C3.7.3.3. Release of C4ISR.

C3.7.3.3.1. Release of Classified Military Data. Interoperable systems that exchange classified military information are subject to a disclosure review and approval as defined in National Disclosure Policy (NDP-1). In addition to classified system hardware and software information, all data flowing between foreign and secure U.S. C4ISR weapon systems is classified. Approvals for disclosure of U.S. classified data that transit over secure coalition networks are required before issuance of LOA and/or P&A data. See Section C3.2.

C3.7.3.3.2. The release and transfer process governing INFOSEC/COMSEC products, information, and techniques to foreign governments or international organizations is an intentionally deliberate decision process undertaken by the Committee on National Security Systems (CNSS) and the NSA Deputy National Manager. These transfers are approved only when there is a clearly defined benefit to U.S. Government (USG) foreign policy, military, intelligence, or economic objectives.

C3.7.3.3.2.1. North Atlantic Treaty Organization (NATO), NATO member nations, Australia, and New Zealand. The release process for INFOSEC/COMSEC products is defined in CNSSP No. 8 (not for public release). INFOSEC/COMSEC products released to these member nations are governed by allied agreements. These, policies and procedures that describe the requirements by which the U.S can provide INFOSEC/COMSEC products, technical security material, information, and techniques.

C3.7.3.3.2.2. International organizations other than NATO, and Non-NATO member nations except Australia and New Zealand. The release process for INFOSEC/COMSEC products is defined in the CJCSI 6510.06 series. A nation's desire to be interoperable with the U.S., or to support the sale of a weapon system is not considered sufficient justification for release. Justification is normally based on Combatant Command (CCMD) requirements to communicate with foreign governments via secure means or USG foreign policy objectives that necessitate release and transfer of U.S. COMSEC. CCMD validation of requirements normally occurs during their bilateral Command and Control Interoperability Board (CCIB) (or like forum) with the Partner Nation. Following validation of the interoperability requirement, the CCMD will initiate the COMSEC Release Request (CRR) process to request a Committee on National Security Systems (CNSS) release decision. There are two types of CRR release approvals, a Release in Principle (RIP) and Release in Specific (RIS).

C3.7.3.3.2.2.1. COMSEC Release in Principle (RIP). A RIP provides a USG policy decision related to release of COMSEC information, products, or services in support of a secure interoperability requirement. A RIP is not an approval to physically transfer any COMSEC product. A RIP is required prior to any detailed discussions with the foreign nation regarding COMSEC products or associated COMSEC information requirements. RIPs are a means to provide proposed solutions to fulfill U.S. secure interoperability requirements.

C3.7.3.3.2.2.2. COMSEC Release in Specific (RIS). A RIS provides USG approval for release of a defined set (quantity and nomenclature) of COMSEC information, products, or services to a Partner Nation. A RIS is required for most all communication devices (secure radios, tactical data links, etc.) included with platform sales. A RIS-General Release (RIS-GR) is a type of release that does not limit the quantity of COMSEC products or tie the approval to a specific weapon system.

C3.7.3.3.2.2.2.1. RIS-GRs may be available for the following COMSEC products:

- AN/PYQ-10 Simple Key Loader (SKL) (all variants)
- Identification Friend or Foe (IFF) Mode 5
- KIK-11 Tactical Key Loader (TKL)
- KIK-30 Really Simple Key Loader (RASKL) products.

C3.7.3.3.2.2.2.1.1. If a country has an approved RIS-GR for a device, the transfer of the device is not limited to a specific quantity when integrated in or used with U.S. manufactured weapon systems. Purchasers may obtain these devices through National Security Agency (NSA) authorized channels without further release approvals. Countries with approved RIS-GRs do not require an NSA Authorization to Sell (ATS) memorandum or e-mail for P&A or LOA staffing packages when the released products are used in/with U.S. weapon systems. Contact DSCA Weapons International C4I Programs office for current RIS-GR country listing (not for public or foreign release).

C3.7.3.3.3. GPS/PPS User Equipment (UE) is not COMSEC or CCI and follows the DoDM O-4650.11 (not for public release) and CJCSI 6510.06 series (not for public release) release processes. The DoD Chief Information Officer (CIO) is the release authority for GPS/PPS UE and GPS anti-jam technology and equipment.

C3.7.3.3.4. Some C4ISR equipment/systems may require additional interagency, service specific, or multi-national release approvals beyond the CNSSP No. 8 (not for public release) or CJCSI 6510.06 series (not for public release) processes. These systems include, but are not limited to: Multifunctional Information Distribution System Low Volume Terminals (MIDS-LVT), Link-22 Beyond Line of Sight Tactical Data Link (BLOS-TDL), GPS/PPS, and radio Waveforms. These additional release requirements may require additional time for release approval; therefore, early planning and coordination with the responsible CCMD is crucial during case development.

C3.7.3.4. <u>INFOSEC/COMSEC P&As and LOAs.</u> The Director, National Security Agency, (DIRNSA) is the National Manager for INFOSEC products to include both external INFOSEC/COMSEC products and embedded cryptographic modules. The Implementing Agency (IA) for INFOSEC/COMSEC products and embedded cryptographic modules is determined by the Acquisition Manager of a particular device. DIRNSA may authorize some NSA-managed INFOSEC/COMSEC products to be included on other IA managed LOAs on a case-by-case basis. Requests for exceptions to allow NSA-managed INFOSEC/COMSEC products on other IA LOAs will not be granted due to the lack of an existing NSA LOA.

C3.7.3.4.1. Special Purpose INFOSEC/COMSEC products ("S" Type COMSEC) are provided to International organizations other than NATO, and non-NATO member nations except Australia and New Zealand on NSA-managed FMS cases only. Requests to allow "S" Type COMSEC equipment on other IA LOAs will not be granted.

C3.7.3.4.2. <u>INFOSEC/COMSEC Validation/Authorization.</u> All IAs, even those responsible for the acquisition of the COMSEC/INFOSEC products and embedded cryptographic modules, must request DIRNSA determination as to whether COMSEC/INFOSEC products and embedded cryptographic modules are releasable and whether they can be included on an

LOA written by an IA other than NSA (exception: see Section C3.7.3.2.2.2.2.1.). Send e-mail request to NSA at FMSLOR@nsa.gov and include a copy of the purchaser's LOR, nomenclature of the COMSEC/INFOSEC products and/or embedded cryptographic modules, quantities, and identify the weapon system or platform in which the COMSEC/INFOSEC equipment will be integrated. When required, DIRNSA will provide a response in the form of an ATS memoranda or e-mail to the IA within 30 days of the request for inclusion in the LOA staffing package.

C3.7.3.4.2.1. A RIP or RIS is required prior to providing a Pricing and Availability (P&A) including COMSEC products to a FMS purchaser. A new RIP or RIS is not required for a P&A if the specific COMSEC/INFOSEC products were previously released (via RIS) to the FMS purchaser for use with a U.S.-manufactured weapon systems AND the COMSEC/INFOSEC products are for use and/or integration into a U.S. manufactured weapon system(s). Address questions concerning previous releases of COMSEC/INFOSEC products to DSCA Weapons International C4I Programs office.

C3.7.3.4.2.2. A RIP is the minimum COMSEC release approval required for Congressional Notifications (CN) containing COMSEC products, unless the product(s) are Major Defense Equipment (MDE). If the COMSEC products are MDE, a RIS is required prior to submitting the CN to identify the specific MDE COMSEC product(s) and quantities in the CN.

C3.7.3.4.2.3. A RIS is required prior to providing a LOA with COMSEC products to a FMS purchaser. Some RIS approvals may include additional instructions for COMSEC/INFOSEC products that require special handling.

C3.7.3.4.3. IAs must verify that the foreign recipient is authorized to receive GPS/PPS UE and anti-jam technology and equipment prior to transfer. If the GPS/PPS UE must operate in PPS mode using encryption, the IA must receive FMS approval from the Air Force (AF) Space and Missile Systems Center Production Corps for Global Positioning Systems and include the approval in the LOA staffing package.

C3.7.3.4.4. Classification of INFOSEC/COMSEC. Some foreign governments may classify their LORs for specific INFOSEC/COMSEC products; however, when possible, classifying the entire FMS case will be avoided. See Section C5.4.10. for more information on classified FMS cases.

2) Add paragraph C3.7.7. and subparagraph as follows:

C3.7.7. Network Enabled Weapons (NEW). NEW are precision-guided munitions that are equipped with datalink radios that allow for re-targeting, altering their respective targeting coordinates, tracking, or passing off control to other weapon systems on the datalink.

C3.7.7.1. A NEW device may employ NSA Type 1 COMSEC encrypted datalink, such as Link-16, or a non-NSA Type 1 COMSEC encrypted datalink, such as Common Datalink (CDL). NEWs with NSA Type-1 COMSEC encryption require COMSEC release approval and NSA ATS for transfer, in addition to any other release approvals and monitoring requirements. See Section C3.7.3. and Section C8.4.1.4.

3) Add C3.7.8. and subparagraphs as follows:

C3.7.8. Cross Domain Solutions (CDS). A CDS is a means of information assurance that provides the ability to manually or automatically access or transfer information between two or more differing security domains. CDS devices are integrated systems of hardware and software that enable the transfer of information among otherwise incompatible security domains or levels of classification. CDS devices may facilitate the connection of U.S. weapon systems acquired by Partner Nations with non-U.S. domains by filtering unauthorized messages and malicious files to protect both U.S. and FMS customer systems, networks, and data.

C3.7.8.1. CDS devices available to FMS purchasers must be tested and certified by the NSA and their transfer requires approval from DIRNSA prior to the USG offering the solutions to the FMS purchaser. IAs must request DIRNSA to determine if the CDS is releasable and whether it can be included on an LOA.

C3.7.8.2. Send requests to NSA FMS Group at FMSLOR@nsa.gov and FMS_P1@nsa.gov and include a copy of the purchaser's LOR, nomenclature of the CDS products, quantities, and identify the weapon system or platform in which the CDS will be integrated. DIRNSA will provide a response in the form of a CDS ATS memoranda or e-mail to the IA within 30 days of the request for inclusion in the LOA staffing package.

4) Update paragraph C4.4.17. as follows:

C4.4.17. Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR). Transfers of U.S. C4ISR to eligible countries and international organizations must support a Combatant Commander's interoperability requirements or U.S. Government policy objectives. A Partner Nation's desire to be interoperable with the United States is insufficient justification for release. Coordination with Defense Security Cooperation Agency (DSCA), the respective CCMD, IAs, the Security Cooperation Organization (SCO) is necessary prior to Partner Nation submitting a C4ISR LOR. See Section C3.7.3. for more information on C4ISR and Table C5.T1C. for more information on processing LORs for C4ISR.

5) Update paragraph C5.1.7. as follows:

C5.1.7. LOR Validation and Acknowledgement of Receipt. Within 5 days of receiving the LOR, the IA will validate the LOR to:

- Ensure that the potential purchaser is an eligible FMS recipient. See Section C4.1.2.
- Ensure that the item sought may be sold. See Section C4.4.
- Ensure that the request was received through proper channels. See Section C5.1.3.
- Determine whether any sanctions exist, that would prevent an LOA from being prepared and/or offered to the purchaser. See Section C6.6. for more information on sanctions.
- Determine whether or not a country or international organization is authorized Dependable Undertaking. The IA will notify the purchaser as soon as possible of the

payment terms available for procurement items to ensure customers have maximum time to make financial arrangements. See Table C4.T2.

Once validated, the IA enters the LOR data in the Defense Security Assistance Management System (DSAMS) as a Customer Request and acknowledges receipt of the LOR to the FMS purchaser. A Customer Request should be created in DSAMS for each LOA document that is prepared. This includes creating separate Customer Requests for multiple LOA documents that are developed based upon one LOR. Creating a separate Customer Request for each LOA document will enable DSAMS to accurately measure the LOA development processing time of each document, to include scenarios where only one of the LOA documents is restated. IAs will forward LORs to other applicable IAs when the recipient IA is not authorized to offer some or all items on the LOR. Example: Air Force (AF) receives an LOR which contains some Communications Security (COMSEC) products which must be offered on a National Security Agency (NSA) LOA, such as "S" type devices. In this instance, the AF will forward the LOR to NSA requesting case development for specific LOR item(s). NSA will provide their Case Identifier to the AF who will notify the FMS purchaser of both case identifiers and LOR details split between the IAs IAW Section C5.1.7.1.1.

6) Update paragraph C6.4.8.2. as follows:

C6.4.8.2. Repair and Return (R&R). R&R is used when a serviceable replacement is not available from stock on hand or due in within a reasonable time, if the FMS purchaser requests R&R of a specific item, or if the item cannot be repaired in the host country. Repair of a purchaser-owned article requires the repairable article be returned in accordance with the terms and conditions listed on the LOA. The FMS purchaser must wait for repair of the article. Supply Discrepancy Reports (SDRs) for non-receipt of R&R items must be submitted in accordance with Section C6.4.10.1.1.

7) Add paragraph C6.4.8.2.1. as follows:

C6.4.8.2.1. A concurrent modification is allowable in instances where a FMS purchaser directs the movement of R&R funds between two or more of their LOAs. See Section C6.7.2.3. and Section C9.11.6. There may be instances where the FMS purchaser needs to utilize R&R funds on one of their LOAs to support the R&R of materiel from another of their LOAs. This is allowable when directed or approved by the FMS purchaser's designated representative, there is available R&R funding to support the additional requirement, and the scope of the R&R line being used is not exceeded. Transportation Plans will be updated as applicable.

8) Update paragraph title C7.3.5.1. as follows

C7.3.5.1. Information Security (INFOSEC)/Communications Security (COMSEC) products.

9) Add paragraphs C7.3.5.1.1. through C7.3.5.1.3. as follows:

C7.3.5.1.1. NATO. NATO member nations, Australia and New Zealand. COMSEC products procured through FMS transfers are titled to those nations.

C7.3.5.1.2. Australia, Canada, New Zealand, and the United Kingdom. Select COMSEC products as defined by NSA may be procured through DCS for those nations. Through ITAR export licensing processes, NSA will authorize the U.S. vendor to sell select COMSEC products. ITAR temporary import licensing applies for repair services under a DCS. See Section C3.3. for ITAR licensing and exemption authorities. FMS support for repair and return allowable, see Section C5.2.1.

C7.3.5.1.3. International organizations other than NATO, and Non-NATO member nations except Australia and New Zealand. Prior to physically receiving any U.S. INFOSEC / COMSEC products or services, the FMS purchaser or recipient must have entered into a bilateral CISMOA or other INFOSEC agreement with the USG via the CCMD. It's recommend that this agreement be initiated before or parallel to LOA development to avoid future shipment delays. The USG retains title to transferred COMSEC equipment in accordance with the bilateral agreement(s) and Committee for National Security Systems (CNSS) release authorization.

10) Update paragraphs C7.13.1. through C7.13.3, and paragraphs C7.13.3.1., and C7.13.3.2. as follows:

C7.13.1. General. A Transportation Plan is required for each LOA containing defense articles that are Classified (CONFIDENTIAL and SECRET), Sensitive (including Controlled Cryptographic Items (CCI), or Arms, Ammunition, & Explosives (AA&E) (Security Risk Categories I - IV) and in which an international transfer occurs. The plan covers all movement including final receipt by the Designated Government Representative (DGR) or other designated representative acting for the DGR. The Transportation Plan format for classified materiel and AA&E, Figure C7.F2., is based on standards agreed to by the Multinational Industrial Security Working Group and NATO. TOP SECRET materiel must always be transferred via government courier. The Transportation Plan format for CCI is based on CNSSI 4001.

C7.13.2. Transportation Plan Preparation. The Transportation Plan is developed by the IA that prepares the LOA in coordination with the FMS purchaser. It is to be submitted to, and approved by, the applicable security authority and accepted by the FMS purchaser, in writing, prior to the movement of the materiel. If Repair and Return items are involved, the Transportation Plan must address all aspects concerning the return of items, including functions to be performed by the sending and receiving entities and notification requirements. Transportation Plans are living documents that must be continually updated.

C7.13.3. Transportation Plan Review. Regardless of custody transfers location, the IA ensures its component Designated Disclosure Authority reviews and approves/disapproves the Transportation Plan if it includes classified materiel. An information copy of the Transportation Plan should be provided to DSCA (Integrated Regional Teams (IRT)).

C7.13.3.1. Classified Requirements. If an FMS freight forwarder or commercial carrier is involved in the transfer of classified materiel, or if classified consignments emanate from a

cleared contractor facility, the Transportation Plan must be provided to the appropriate DCSA Field Activity. The Defense Counterintelligence and Security Agency verifies the security clearance of FMS freight forwarders, as well as any industry appointed courier or escort. DCSA oversees and enforces all security measures implemented by cleared contractors in safeguarding classified information pursuant to the National Industrial Security Program Operating Manual (NISPOM), regardless of the manner through which contractors have taken possession of the classified material. If the Transportation Plan results in inconsistencies with the requirements of the NISPOM or with previous agreements between the implementing governments concerning security procedures, the IA, with assistance and guidance from DCSA, will make necessary changes and resolve the inconsistencies with the Designated Security Authorities of the implementing governments. DSCA (Strategy, Plans, and Policy Directorate (SPP)), and Defense Technology Security Administration (DTSA) (Director, International Engagement Directorate) will be notified by DCSA if the IA and DCSA are not able to resolve matters satisfactorily. Only cleared carriers qualified by Surface Deployment and Distribution Command or Protective Security Service will be used for shipments internationally. International transfer of classified material should only be made using ships, aircraft or other carriers that are:

- Wholly owned or chartered by the USG, or under U.S. Registry;
- Owned or chartered by, or under the registry of the recipient government; or
- Carriers other than those described that are expressly authorized to perform this function in writing by DTSA (Director, International Engagement Directorate), and the security authorities of the foreign government involved.

C.7.13.3.1.1. For classified materiel the FMS Case Manager and supporting security office should coordinate with DCSA and other government security and Customs authorities to ensure that the proper security arrangements are made to facilitate transfers through port and carrier security.

C7.13.3.2. AA&E Requirements. Reviews of Transportation Plans for unclassified shipments that are Sensitive or AA&E are conducted by the IA. DCSA does not require copies.

11) Add paragraphs C7.13.3.3., and C7.13.3.3.1. as follows:

C7.13.3.3. CCI Requirements. CCI are unclassified but controlled secure telecommunications equipment and associated cryptographic assemblies, components or other hardware or firmware products that perform a critical COMSEC function. Un-keyed CCI is unclassified and shipment requires a Transportation Plan as specified in Figure C7.F4. DSCA must approve an exemption to policy to ship keyed CCI - utilize the Transportation Plan requirements in Figure C7.F3. and Figure C7.F4. for these approved exemptions.

C7.13.3.3.1. Transportation Plans for CCI must include required information for the initial delivery, returns for repair, and are updated when demilitarization functions are confirmed, all which requires the transfer of the item from the authorized shipping COMSEC Custodian/Manager to the recipient's COMSEC Custodian/Manager. The SF-153 COMSEC

Material Report is used by the shipping COMSEC Custodian/Manager to document the transfer of COMSEC products. The receiving COMSEC Custodian/Manager notifies the shipping COMSEC Custodian/Manager upon receipt of the item(s) by signing and returning the SF-153 to the shipping COMSEC Custodian/Manager. Transportation Plan approval will be dependent on an implemented CISMOA or other agreement; see Section C7.3.5.1.3.

12) Update paragraph C7.13.4. as follows:

C7.13.4. Transportation Plan Usage. Once approved, a Transportation Plan becomes an integral part of the LOA and is available for review by U.S. Customs and security officials when exported. A Transportation Plan must be updated regularly. FMS purchasers are responsible for ensuring that their FMS freight forwarders have copies when involved with exports. When possible, the details of the Transportation Plan should be included in the DoD Service Contract for appropriate movement of the cargo to its destination. Contracts should also include the Security Risk Category and National Stock Number, as appropriate, so shipments are properly marked and utilize the necessary protective services.

13) Add new figure at C7.F4. as follows:

Figure C7.F4. CCI Transportation Plan Requirements

CNSSI No. 4001 (not for public release) requires the Transportation Plan for Controlled Cryptographic Items (CCI) shipments and it becomes an integral part of the delivery and custody of CCI. Shipment of keyed CCI is typically not authorized. See Section C7.13.3.3. If CCI must be ship keyed, then the standard Transportation Plan must be must be utilized, See Figure C7.F3. and in addition include the following CCI Transportation Plan requirements.

The CCI shipping activity must provide the intended recipient with advance notification via a Notice of Availability (NOA) for the impending shipment. Report of Shipment (REPSHIP) procedures will be followed; see the DTR Part II Chapter 205. This advance notification will help to readily identify any shipment that may be unduly delayed or lost enroute. The Recipient COMSEC Manager must sign and return the SF-153 to the shipper within 48 hours of receipt of material. At a minimum, the Transportation Plan for CCI will include the following information prior to shipment:

a) All transportation of CCI must provide In-Transit Visibility (ITV) and reasonable protection against theft or loss of the materiel while it is in transit. ITV is the ability to track the status and location of shipments from origin to consignee or destination. Include website and/or phone number for shipment ITV queries.

b) A description of the materiel together with a brief narrative as to where and under what circumstances transfer of custody occurs;

c) Transportation method utilized or overview:

d) Transportation Control Number, Shipper Reference Number, and/or Bill of Lading

e) Shipment origin information (COMSEC Account Number and location)

f) Trans-shipment information (location, city, country, etc.)

g) Destination information (COMSEC Account Number and location)

h) Contact information for individuals aware of shipment.

14) Renumber original figure C7. F4. to C7.F5.

15) Renumber original figure C7.F5. to C7.F6.

16) Replace paragraph C7.15.4. and all subparagraphs as follows:

C7.15.4. CCI. CCI recipients are permitted to move CCI (to include external peripheral/support equipment) through FMS freight forwarders or the Defense Transportation System (DTS), provided that in-transit visibility and reasonable protection against theft and loss is maintained at all times. See Figure C7.F4. The FMS purchaser may impose more stringent controls on shipment of CCI when transporting outside the United States.

C7.15.4.1. Packaging requirements. Un-keyed CC must be packaged for shipment in any manner that provides sufficient protection from damage, and provides evidence of any attempt to penetrate the package while the material is in transit.

C7.15.4.1.1. In order to conceal the sensitive nature of the shipment, packages containing CCI must not be externally marked as CCI or show the item description (nomenclature) of the equipment being shipped. For exterior container documentation purposes, CCI is are considered controlled and sensitive items (e.g., MIL-STD-129, paragraph 5.3.3.).

C7.15.4.1.2. CCI must only be shipped to authorized activities. Packages must be addressed in a manner that will ensure delivery of the material to an organization with an individual designated to accept custody for it at the recipient activity. An individual's name should not be used in the address; rather a functional designator should be used (e.g., an office symbol, a MAPAC, or a COMSEC Material Control System (CMCS) account number).

17) Update and move subparagraph 7.15.4.2.1.1. to paragraph C7.6.2.5 as follows:

C7.6.2.5. Next Generation Delivery Services (NGDS). NGDS is a USG-wide contract for domestic and international express small package delivery services, and domestic ground small package delivery services. NGDS provides international commercial express delivery for unclassified shipments up to and including 300lbs with time-definite, door-to-door pick-up and delivery, and accurate in-transit visibility service for DOD and USG Civil agencies. U.S. Government shippers must establish an account and arrange individual shipments. For additional guidance on the use of NGDS, see Chapter 202 of the DTR. All questions related to NGDS should be directed to the TRANSCOM J4-L.

18) Update and move subparagraph 7.15.4.2.1.2. to paragraph C7.6.2.6 as follows:

C7.6.2.6. Defense Courier Service (DCS). DCS provides secure, timely, and efficient end-to-end global distribution of classified and sensitive material for the United States and its

Partners and Allies. It is an established courier network to transport qualified materiel. DCS is recommended primarily for circumstances where the USG retains title to the materiel during transit. For additional information on the use of DCS, contact TRANSCOM's Defense Courier Division and See Chapter 205 of the DTR.

19) Renumber original paragraph C7.6.2.5. to C7.6.2.7.

20) Renumber original paragraph C7.6.2.6. to C7.6.2.8.

21) Update paragraph C8.4.1.4. as follows:

C8.4.1.4. All COMSEC products require Enhanced End Use Monitoring (EEUM) and is documented in COMSEC management systems other than Security Cooperation Information Portal (SCIP). Transferred COMSEC products are changed from EEUM to Routine EUM in SCIP (unless EEUM for additional reasons other than COMSEC) but retain the EEUM and documentation requirements, as follows:

22) Add subparagraphs C8.4.1.4.1 through C8.4.1.4.4. and paragraph C8.4.1.5. as follows:

C8.4.1.4.1. The EEUM of COMSEC products purchased by Partners or Allies and retained by U.S. government or industry for testing, integration, etc., is performed by the U.S. government or industry's respective COMSEC safeguarding, accountability, and reporting procedures.

C8.4.1.4.2. The EEUM of COMSEC products transferred to NATO, NATO member nations, Australia, and New Zealand is performed by recipient nation IAW their COMSEC policies and regulations.

C8.4.1.4.3. The EEUM of COMSEC products transferred to International organizations other than NATO and non-NATO member nations except Australia and New Zealand who have signed a Communication Interoperability and Security Memorandum of Agreement (CISMOA) or like agreement is accomplished by the FMS-funded U.S. COMSEC custodians.

C8.4.1.4.4. The EEUM of COMSEC products transferred to non-NATO member nations who have not signed a CISMOA or like agreement is accomplished by the SCOs and reported to their respective theater CCMD Theater COMSEC Account. CCMDs must ensure SCOs perform the required COMSEC security and accountability checks.

C8.4.1.5. Network Enabled Weapons (NEW) with NSA Type 1 COMSEC encrypted datalink require COMSEC EUM IAW C8.4.1.4. and may require additional monitoring requirements. See Table C8.T4.

23) Add paragraph C8.8.5. and subparagraph C8.8.5.1. as follows:

C8.8.5. Demilitarization of COMSEC products must be conducted by a NSA approved COMSEC demilitarization/destruction facility. Service IAs will utilize their service COMSEC authority disposition guidance for demil of COMSEC products via FMS.

COMSEC products procured/transferred via FMS must be returned and demilitarized via FMS.

C8.8.5.1. Only NSA is authorized to demilitarize "S" type COMSEC products.

24) Add the following terms to SAMM Glossary:

Term	Definition
Information Security (INFOSEC)	The 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 threat. INFOSEC is applied through the application of Cybersecurity and Communications Security (COMSEC).
Communications Security (COMSEC)	The measures and controls taken to deny unauthorized persons' information derived from telecommunications and other information systems, and technologies necessary to ensure the authenticity of such communications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. Secure telecommunication or information system cryptographic components are the primary COMSEC products for transmission security and commonly called COMSEC devices or products. COMSEC devices are designated Controlled Cryptographic Items (CCI).
Controlled Cryptographic Items (CCI)	CCIs are devices that embody cryptographic logic or other cryptographic design, but do not perform the entire Communications Security (COMSEC) function. CCIs are dependent upon host equipment or assemblies to complete and operate COMSEC functions. Un-keyed CCI is unclassified. An item may be designated CCI because its entire component is controlled (e.g. Inline Network Encryptor (INE)), or because the item contains an embedded cryptographic National Security Agency (NSA) Type-1 certified module to encrypt/de-encrypt information (e.g. secure radio).
Release In Principle (RIP)	A Communications Security (COMSEC) RIP is 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 product. A RIP is required prior to any detailed discussions with the foreign nation regarding COMSEC products or associated COMSEC information requirements. RIPs are a means to support requirements definition

Term	Definition
	for proposed solutions to fulfill U.S. secure interoperability requirements.
Release in Specific (RIS)	A Communications Security (COMSEC) RIS is a USG approval for release of a defined set (quantity and nomenclature) of COMSEC information, products, or services to a Partner Nation.