DEFENSE SECURITY COOPERATION AGENCY

WASHINGTON, DC 20301-2800

MAR 2 3 2007

In reply refer to:
I-06/016022-PGM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy for Transfers Involving Command, Control, Communications,
Computer, Intelligence, Surveillance and Reconnaissance (C4ISR),
DSCA Policy 06-54 [SAMM E-Change 59]

REFERENCE: DSCA Policy 06-13, SAMM E-Change 44, March 16, 2006 (Rescinded)

Attached is the revised update to Chapters 3, 4, and 5 of the SAMM regarding the
policy for transfers of C4ISR capabilities. The guidance defines C4ISR and the release
process, identifies roles and responsibilities of key players involved in the C4ISR
process, and provides detailed procedures for C4ISR release and transfer to FMS
purchasers.

Table C3.T4. of the SAMM provides detailed information relating to each
organization involved in C4ISR transfers and its responsibilities throughout the process.
DSCA will establish training for these organizations to ensure each is fully aware of and
familiar with the functions required during the three phases of this program.

This change will be included in the automated version of the SAMM found on the
DSCA Web Page as SAMM E-Change 59. If you have any questions concerning this
policy, please contact Mr. Gregg Bergersen, DSCA/PGM/WPN, at (703) 604-0423,
e-mail: gregg.bergersen@dsca.mil. For questions regarding the SAMM, please contact
Ms. Kathy Robinson, DSCA/STR/POL, at (703) 601-4368 or e-mail:
kathy.robinson@dsca.mil.

Attachment
As stated

JEFFREY B. KOHLER
LIEUTENANT GENERAL, USAF
DIRECTOR

DISTRIBUTION LIST

DEPUTY ASSISTANT SECRETARY OF THE ARMY
DEFENSE EXPORTS AND COOPERATION (DASA-DEC)
DEPARTMENT OF THE ARMY

DEPUTY ASSISTANT SECRETARY OF THE NAVY
INTERNATIONAL PROGRAMS (NAVIPO)
DEPARTMENT OF THE NAVY

DEPUTY UNDER SECRETARY OF THE AIR FORCE
INTERNATIONAL AFFAIRS (SAF/IA)
DEPARTMENT OF THE AIR FORCE

DIRECTOR, DEFENSE LOGISTICS AGENCY

DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

DIRECTOR, DEFENSE REUTILIZATION AND MARKETING SERVICE

DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY

DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

DIRECTOR, DEFENSE LOGISTICS INFORMATION SERVICE

DEPUTY DIRECTOR FOR INFORMATION ASSURANCE,
NATIONAL SECURITY AGENCY

DEPUTY DIRECTOR FOR SECURITY ASSISTANCE,
DEFENSE FINANCE AND ACCOUNTING SERVICE - DENVER CENTER

cc: STATE/PM-RSAT
     USDP/ISP
     DISAM
     USASAC
     SATFA TRADOC
     NAVICP
     NETSAFA
     AFSAC
     AFSAT
     JFCOM
     SOCOM
     EUCOM
     CENTCOM
     NORTHCOM
     PACOM
     SOUTHCOM

Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Policy – SAMM E-Change 59

1. Replace Chapter 3, Section 3 and all sub paragraphs with the following.

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

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

C3.3.2. C4ISR Release Process.

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

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

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

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

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

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

Table C3.T4. C4ISR Responsibilities

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

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

C3.3.5. <u>C4ISR Planning Process - Three-Phased Approach (3PA)</u>.   To the greatest extent possible, C4ISR foreign requirements are addressed from a joint service perspective.   Before a C4ISR LOR is submitted, pre-coordination with DSCA (Operations and Programs Directorates), the respective COCOM, potential Implementing Agencies, the SAO, and the foreign purchaser is recommended. Through this pre-LOR coordination, DSCA determines whether the COCOM supports the transfer, identifies releasability challenges, and designates the lead Implementing Agency and, where applicable, supporting Implementing Agencies in advance of receiving the C4ISR LOR (see C5.1.4.3.5). DoD encourages the use of a 3PA to plan C4ISR programs, as outlined below. Separate LORs are normally submitted for each individual phase of the 3PA.

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

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

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

C3.3.6. <u>INFOSEC FMS Case Processing</u>. NSA is the Implementing Agency for INFOSEC products, to include both external INFOSEC equipment and embedded cryptographic modules. NSA may grant exceptions for other Implementing Agencies to establish FMS cases that include INFOSEC products embedded in weapons and communication systems. The association of a specific INFOSEC product with a foreign government may be classified; however, classifying the entire FMS case will be avoided, when possible.   See Chapter 5, C5.4.11. for more information on classified FMS cases. For more information on what equipment may be transferred, contact DSCA (Programs Directorate).

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

2. Insert the following new section in Chapter 4:

C4.3.17. <u>Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR)</u>. Transfers of U.S. C4ISR to eligible countries and international organizations must support a U.S. Combatant Commander's (COCOM) interoperability requirements. A purchaser's desire to be interoperable with the United States is insufficient justification for release. DoD encourages the use of a Three-Phased Approach to plan C4ISR programs. Before a C4ISR Letter of Request (LOR) is submitted, pre-coordination with DSCA, the respective Combatant Command, Implementing Agencies, the SAO, and the foreign purchaser is required. See Chapter 3 for more information on C4ISR and Chapter 5 for more information on processing LORs for C4ISR.

3. Insert the following new section in Chapter 5:

C5.1.4.3.6. <u>LORs for Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR)</u>. Upon receipt of the LOR, the Implementing Agency forwards the LOR for C4ISR to DSCA (Operations Directorate). After DSCA and the Implementing Agency validate and review the LOR in accordance with subparagraphs C5.1.4.1., C5.1.4.2., and C5.1.4.4., DSCA determines if an LOR Advisory is required.