



DEFENSE SECURITY COOPERATION AGENCY

WASHINGTON, DC 20301-2800

MAR 16 2006

In reply refer to:
I-05/014306-STR

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy for Transfers Involving Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR), DSCA Policy 06-13 [SAMM E-Change 44]

Effective immediately, Chapter 3 of the Security Assistance Management Manual (SAMM) is updated to include policy for transfers involving C4ISR. The attached addition identifies planning guidance, eligibility requirements, responsibilities, and procedures for C4ISR release and transfer.

This change will be included in the automated version of the SAMM found on the DSCA Web Page as SAMM E-Change 44. If you have any questions concerning this policy, please contact Mr. Gregg Bergersen, DSCA/PGM/WPN, at (703) 604-0243, e-mail: gregg.bergersen@dsc.mil. For questions regarding the SAMM contact Ms. Kathy Robinson, DSCA/STR/POL, at (703) 601-4368 or e-mail: kathy.robinson@dsc.mil.

A handwritten signature in black ink, appearing to read "J. B. Kohler".

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 44

Insert the following new section in Chapter 3 and renumber subsequent sections and paragraphs.

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. This section focuses on C4ISR systems that process and protect classified information for military operations or homeland security purposes. 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.

C3.3.2. C4ISR Eligibility Requirements. Transfers of U.S. C4ISR systems to eligible countries and international organizations must support a U.S. Combatant Commander's (COCOM) interoperability requirements. The COCOM must require the transfer of the capability. A purchaser's desire to be interoperable with the United States is insufficient justification for release. Additionally, the purchaser must negotiate and sign a Communication Interoperability and Security Memorandum of Agreement (CISMOA) or other bilateral INFOSEC agreement (e.g., COMSEC MOU, INFOSEC Equipment Agreement) with the COCOM, prior to physically receiving any U.S. INFOSEC products or services associated with a secure C4ISR system. The COCOM and the purchaser's authorized official sign the bilateral CISMOA unless covered under a multilateral treaty and/or separate bilateral agreements, which negates the requirement to sign a CISMOA. The COCOM may negotiate exceptions to a CISMOA on a case-by-case basis. A purchaser should be approved for access to classified C4ISR data and INFOSEC prior to submitting a C4ISR Letter of Request (LOR).

C3.3.3. C4ISR Responsibilities. Table C3.T4. lists organizations and their C4ISR responsibilities. Representatives from the COCOM, DSCA, Chairman, Joint Chiefs of Staff, Office of the Secretary of Defense (OSD) Networks and Information Integration (NII), Implementing Agencies, and National Security Agency (NSA) comprise the membership of the C4ISR Oversight/Steering Group.

Table C3.T4. C4ISR Responsibilities

Organization	Responsibility
Security Assistance Organization (SAO)	<ul style="list-style-type: none"> - Informs host country of the requirement for COCOM sponsorship of requests for INFOSEC-enabled C4ISR systems - Informs host country of the COCOM point of contact for international C4ISR requirements prior to submitting the LOR to DSCA for purchase - Promotes the C4ISR three-phased approach (see paragraph C3.3.4 for more information), to assist the country with planning and budgeting for secure interoperable U.S. C4ISR systems - Forwards C4ISR LORs to COCOM J3, J4, J5, J6, J9, and DSCA
COCOM	<ul style="list-style-type: none"> - Establishes interoperability requirement for specific C4ISR capabilities requiring INFOSEC products and services - Initiates CJCSI 6510.06 (reference (ap)) INFOSEC release process - Following delegation of authority from the Chairman, Joint Chiefs of Staff and NSA, negotiates and signs the CISMOA or appropriate bilateral INFOSEC agreement governing the transfer of INFOSEC products and services to non-NATO (excluding Australia and New Zealand) nations - Negotiates exceptions to CISMOAs - Leads Concept of Operations (CONOPS) Working Integrated Process Team (WIPT) - Member of C4ISR Oversight/Steering Group
Implementing Agencies	<ul style="list-style-type: none"> - Lead Implementing Agency generates Price and Availability (P&A) data/FMS case - Lead Implementing Agency funds other participating Implementing Agencies and organizations (COCOMs) and maintains funding to support administration costs with FMS case funds - Assigns In Process Team (IPT) leads for each warfare specialty - Member of the C4ISR Oversight/Steering Group
DSCA	<ul style="list-style-type: none"> - Reviews C4ISR LORs and, as appropriate, assigns lead Implementing Agency - Monitors planning activities - Member of the C4ISR Oversight/Steering Group - Provides input and review of C4ISR planning process
Chairman, Joint Chiefs of Staff	<ul style="list-style-type: none"> - Validates COCOM interoperability requirements associated with the request for U.S. INFOSEC products and services - Delegates final authority to COCOM to negotiate and conclude the CISMOA - Member of the C4ISR Oversight/Steering Group
OSD	<ul style="list-style-type: none"> - OSD(NII) provides input and review of planning process - Member of C4ISR Oversight/Steering Group
NSA	<ul style="list-style-type: none"> - 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 put specific INFOSEC products and services on Military Department FMS cases (see National COMSEC Instruction (NACSI) 6001 (reference (am))) - Member of the C4ISR Oversight/Steering Group
Purchaser	<ul style="list-style-type: none"> - Signs a bilateral CISMOA or other binding INFOSEC agreement - Funds, as appropriate, an FMS case for a dedicated INFOSEC facility, staffing by 2 U.S. accredited COMSEC custodians, and Phases 1, 2, and 3 deliverables of the C4ISR process (see C3.3.4.)

C3.3.4. C4ISR Planning Process - Three-Phased Approach. DoD encourages the use of a Three-Phased Approach to plan C4ISR programs. Phases 1 and 2 of this approach typically require inputs and reviews from the COCOM, Chairman, Joint Chiefs of Staff, OSD (NII), DSCA, Implementing Agencies, and NSA. Phase 3 involves execution of FMS cases for various elements of a purchaser's C4ISR infrastructure. Monitoring occurs through existing international forums such as COCOM Security Cooperation Conferences and Command and Control Interoperability Boards, Program Management Reviews, or C4ISR Oversight/Steering Group meetings. The C4ISR Oversight/Steering Group consists of representatives from the COCOM, DSCA, Chairman, Joint Chiefs of Staff, OSD (NII), Implementing Agencies, and NSA. C4ISR Oversight/Steering Group meetings are called, as needed, to address policy, operational or acquisition issues for Phases 1 and 2 programs. To the greatest extent possible, C4ISR foreign requirements are addressed with a joint service approach.

C3.3.4.1. Phase 1. The deliverables of Phase 1 include a Concept of Operations (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. Before submitting an LOR for a complex, secure C4ISR system, purchasers are encouraged to establish an FMS case for C4ISR planning that explores the intended CONOPS and develops an overarching C4ISR architecture. A dedicated FMS planning case funds a U.S. tri-Service, joint effort that ensures efficient, interoperable, and economical technical solutions that enhance interoperability with U.S. forces. If the purchaser declines an FMS planning case, the FMS case to support the C4ISR system sale should include provisions to address interoperability, CONOPS, and C4ISR architecture development. LORs for secure C4ISR systems (e.g., studies, planning, training, communications hardware and software, COMSEC facilities, and COMSEC custodians) should be forwarded to DSCA and the COCOM J3, J4, J5, J6, and J9 to determine if the request supports a COCOM interoperability requirement. This process applies both to new purchases of C4ISR systems, as well as to follow-on purchases of the same C4ISR systems. During this stage, if INFOSEC devices or information are required, a COMSEC Release Request (CRR) is sent to the COCOM by the U.S. entity or sponsor for endorsement. The inclusion of INFOSEC products or associated COMSEC information in weapons, communications, or other major defense systems, to provide a complete FMS package, is not an acceptable justification for seeking release of those products or information. If the need for these products is an integral part of a communications or weapon system, the COCOM's Combined COMSEC Manager at the COCOM J3/J6/J9 should be contacted to discuss the requirement and follow-on actions. Release approval for countries other than NATO/NATO nations and Combined Communications-Electronics Board nations for INFOSEC products must be obtained through the CJCSI 6510.06 (reference (ap)) process before an FMS case can be initiated. DSCA also reviews the LOR to determine its match with COCOM, Chairman, Joint Chiefs of Staff, NSA, and OSD policy requirements prior to assigning a lead Implementing Agency. The Implementing Agency coordinates activities and produces recommendations. The Implementing Agency, in concert with the supporting Services and agencies, present to the C4ISR Oversight/Steering Group the joint program management concept for executing Phase 1 and Phase 2 programs 3-5 months after case signature.

C3.3.4.2. Phase 2. The primary deliverable of Phase 2 is a Procurement Plan. It is generated within 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. The Procurement Plan provides a “total package” of options and recommendations with associated costs, schedules, and risk impacts to the purchaser. Other tasks include definition of information exchange requirements, refinement of high-level architecture, and initiation of C4ISR training. These activities are funded through an FMS case. Due to the joint nature of these programs, DSCA will assign an Implementing Agency to lead this effort. The lead Implementing Agency generates the P&A data/FMS case after coordinating and integrating other Implementing Agency inputs into the document.

C3.3.4.3. Phase 3. Phase 3 implements the Phase 2 procurement strategy through direct commercial sales, FMS, 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)).

C3.3.5. C4ISR Funding. Planning for C4ISR interoperability will take place whether there is a dedicated FMS planning case or as part of a larger systems acquisition program. The lead Implementing Agency for this joint effort assigns IPT leads for each warfare specialty and ensures other participating Implementing Agencies and organizations are funded by the planning case on a pro rata basis. For example, if the U.S. IPT lead (with input from the Purchaser as appropriate) determines that 40% of its Phase 1 efforts are concentrated on Air Force programs, 40% on Army programs, and 20% on Navy programs, the Phase 1 Implementing Agency funding allocations should generally reflect these percentages. The lead Implementing Agency maintains funding to support administration costs.

C3.3.6. INFOSEC FMS Case Processing. FMS programs that support secure interoperability with U.S. forces invariably include some INFOSEC products. NSA is the Implementing Agency for FMS cases for INFOSEC products, to include both external INFOSEC equipment and embedded cryptographic modules. NSA may grant limited exceptions for another Implementing Agency 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/Weapons Division).

C3.3.7. FMS Case for INFOSEC Custodians. C4ISR purchasers may be required to fund an FMS case to purchase a dedicated INFOSEC account and 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. The host country forwards the LOR for the INFOSEC facility/custodians to DSCA to determine the appropriate lead Implementing Agency. NSA and the COCOM may assign additional duties to INFOSEC custodians. A lead Implementing Agency will be assigned responsibility for managing the FMS case and ensuring custodians are responsive to the COCOM and the U.S. Embassy to meet all U.S. secure interoperability requirements.

C3.3.8. C4ISR Release Process.

C3.3.8.1. 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 classified coalition operational data and/or U.S. Order of Battle data are required before a C4ISR system can be offered via FMS channels (see section C3.5.).

C3.3.8.2. INFOSEC Release. The release process for INFOSEC products is defined in CJCSI 6510.06 (reference (ap)). With two exceptions (see paragraph C3.3.8.3 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.

C3.3.8.3. Global Positioning System/Precise Positioning Service (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 as needed through NSA-authorized channels.

C3.3.8.4. Bilateral INFOSEC Agreement Signature. The 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.