C13. CHAPTER 13

DSCA MANAGEMENT INFORMATION SYSTEMS AND REPORTS

C13.1. INFORMATION TECHNOLOGY (IT) GOVERNANCE BOARD AND CHANGE REVIEW BOARD (CRB)

The Information Technology (IT) Governance Board and the IT Change Review Board (CRB) review all new IT system enhancements and/or system developments financed by DSCA managed funding (e.g., Foreign Military Sales, Foreign Military Financing, Operation & Maintenance, etc.). These review boards ensure that the integrity of the existing IT systems is maintained and that future system developments are evaluated for tri-service applicability, cost effectiveness, and overall benefit to the security cooperation community. The establishment of the IT Governance Board and the designation of the Pre-Certification Authority (PCA) is consistent with the Under Secretary of Defense (Acquisition, Technology, and Logistics) memorandum, June 02, 2005, subject: "Investment Review Process Overview and Concept for Operation for Investment Review Boards" (reference (di)), which implements 10 U.S.C. 2222 (reference (dj)).

C13.1.1. Information Technology (IT) Governance Board Membership. The IT Governance Board consists of members from each of the following organizations: Defense Security Cooperation Agency (DSCA), the Department of the Army, the Department of the Navy, and the Department of the Air Force. The Director, DSCA, serves as the IT Governance Board chairperson. The Deputy Director, DSCA, is the Pre-Certification Authority responsible for reviewing all new IT system enhancements and/or system developments that are financed with DoD appropriated funds exceeding $1M and is also a member of the IT Governance Board. The IT Governance Board members are allowed one additional representative to accompany them to IT Governance Board meetings. Additionally, the following representatives from DSCA attend these meetings to serve as advisors to the IT Governance Board: Principal Director, Strategy; Principal Director, Information Technology; Principal Director, Business Operations; and IT CRB Chairperson.

C13.1.2. Information Technology (IT) Governance Board Function. The IT Governance Board meets on a quarterly basis to review and approve all requests for new IT system enhancements and/or system developments or on an ad hoc basis to discuss relevant IT issues. The IT Governance Board ensures all proposed IT system enhancements and/or system developments are necessary and do not exceed current IT budget levels and/or future Program Objective Memorandum (POM) levels. All new IT system enhancements and/or system developments reviewed and prioritized may not be funded. The IT Governance Board makes the determination of which new IT system enhancements and/or system developments to approve and fund within existing resources allocated to support IT for the security cooperation community. The IT Governance Board only reviews repair/maintenance requests exceeding $500K.

C13.1.3. <u>Information Technology (IT) Change Review Board Membership</u>. DSCA (Strategy Directorate/Policy Division) chairs the IT CRB along with members from the Department of the Army, the Department of the Navy, and the Department of the Air Force, who serve as their Service's focal point for submitting new requests for IT system enhancements and/or system developments

C13.1.4. <u>Information Technology (IT) Change Review Board (CRB) Function.</u> The IT CRB conducts the initial review of new IT system enhancement and/or system development requests and provides recommendations to the IT Governance Board. All users of the various IT systems are encouraged to submit recommended enhancements through their designated IT CRB member. These enhancements include fixes to perceived problems with IT systems or requests for additional and/or enhanced functionality. The IT CRB only reviews repair/maintenance requests exceeding $500K. Reviews will take place electronically to the extent possible.

C13.1.5. <u>Information Technology (IT) Governance Board and Change Review Board (CRB) Review Process.</u> Table C13.T1. summarizes the IT Governance Board and CRB process.

Table C13.T1. Information Technology (IT) Governance Board and
Change Review Board (CRB) Review Process

Step	Action
1 User submits request(s)	Using Figure C13.F1., the user submits all requests to his or her designated IT CRB member, who forwards all requests for new IT system enhancements and/or system developments to the IT CRB for review. All requests for new IT system enhancements and/or system developments that exceed $500K may require an independent business case analysis as determined by the IT CRB.
2 Review by the IT point of contact or Program Manager	Prior to submission of any IT system enhancement and/or IT system development requests to the IT CRB for review, the IT CRB member must have the appropriate IT point of contact or Program Manager provide a recommendation on the level of effort, technical feasibility, and technical benefit of the proposed IT system enhancement and/or system development. New IT system enhancement and/or system development requests that have not been reviewed by the appropriate IT point of contact or Program Manager will be sent back to the IT CRB member for proper vetting. The applicable IT point of contact or Program Manager maintains and tracks all approved IT enhancements for their IT system and provide updates to the IT CRB.
3 Submissions forwarded to IT CRB chairperson	Upon receipt of the IT point of contact or Program Manager's recommendation, the IT CRB member forwards the request to the IT CRB chairperson for review by the IT CRB.
4 Review by IT CRB members	On a quarterly basis, the IT CRB chairperson consolidates all requests for IT system enhancements and/or system developments and disseminates them to the IT CRB members for review and prioritization. The IT CRB members prioritize each request from a highest to lowest priority using the numbering system (i.e., 1-10) with one being the highest priority. Each request is ranked on its own merit. If an IT CRB member rejects a request this must be indicated as part of the ranking along with the rationale for the rejection. All rejections are discussed by the IT CRB and returned to the submitter along with the rationale for the rejection. If an IT CRB member has questions or concerns regarding a specific request, the IT CRB member notifies the IT CRB chairperson prior to providing the rankings who will determine whether a meeting is required to address the issue. The IT CRB member is responsible for clarifying or adjudicating policy-related questions or requests for policy changes with applicable policy owners. If the requested IT system enhancement and/or system development involves policy changes (e.g., a requested change to or re-interpretation of existing policy), the IT CRB member must return the request to the submitter with a recommendation to contact his or her own policy office for resolution prior to resubmitting the request.

Step	Action
5 Consolidated list forwarded to the IT Governance Board	Upon receipt of the IT CRB members' recommendation of the IT system enhancements and/or system developments, the IT CRB chairperson consolidates the recommendations into a list to be forwarded to the IT Governance Board chairperson (noting all rejections received). For new IT system developments, the IT CRB chairperson notifies the appropriate IT point of contact or Program Manager to prepare a brief for the upcoming IT Governance Board meeting on the proposed IT system development.
6 Review by IT Governance Board	The IT Governance Board meets quarterly to discuss the IT system enhancements and/or system developments on the consolidated list received from the IT CRB or on an ad hoc basis to discuss relevant IT issues. For new IT system developments, the IT point of contact or Program Manager (after Implementing Agency chief information officer review) briefs the IT Governance Board on the proposed IT system's capabilities and overall benefit to the security cooperation community. After review of the consolidated list of IT system enhancements and/or system developments, the IT Governance Board chairperson renders a decision that is recorded and disseminated to the IT CRB chairperson for appropriate action by the applicable IT point of contact or Program Manager. For new IT system developments, the IT point of contact or Program Manager must obtain the IT Governance Board's approval in time for the annual DSCA POM and budget process.

Figure. C13.F1. – Information Technology (IT) Governance Board and
Change Review Board (CRB) Evaluation Form

Information Technology (IT) Governance Board and Change Review Board (CRB) Evaluation Form		
Project #:		
Title/Description:		
Submission Date:		**Submitted By Agency/Service:**
EVALUATION CRITERIA	**Level of Effort:**	
	Feasibility:	
	Estimated Cost:	
	Return on Investment:	
	Volume of Use:	
	User Impact:	
	Impact to Existing Systems:	
	Proposed Process Improvement / Efficiency:	
	Benefit to the Security Cooperation Community:	
For IT Governance Board and Change Review Board Use Only		
IT CRB Recommendation/ Prioritization		
IT Governance Board Decision Approve/ Disapprove:		
Pre-Certification Authority (PCA) Approval: (if applicable)		
* Submitters are not limited to the space allotted on this form and are encouraged to provide as much detailed information as possible.		

C13.2. <u>DEFENSE SECURITY ASSISTANCE MANAGEMENT SYSTEM (DSAMS)</u>

C13.2.1. <u>DSAMS Business Function.</u> DSAMS functions include recording receipt of Letters of Request (LORs); creating Letters of Offer and Acceptance (LOAs), Amendments, Modifications, Price and Availability (P&A) data, Leases, and Pen and Ink changes; and case implementation. When the case is implemented, case data is passed to MILDEP legacy systems for case execution. See Chapters 5 (FMS Case Development) and 6 (FMS Case Implementation, Execution and Closure) for additional information for case development and execution. As a result of the deployment of the DSAMS Training Module in October 2006, DSAMS has now replaced US Army and US Navy legacy systems as the system of record for the US Army's and US Navy's execution of foreign military training under the applicable Security Cooperation programs. See Chapter 10 (International Training) for additional information on the foreign military training policies DSAMS was built to support. The interfacing Security Assistance Network (SAN), Training Management System (TMS), International Military Student Office (IMSO) Web, and Security Cooperation Organization (SCO) Web have been significantly enhanced in accordance with the DSAMS Training Module deployment. The US Air Force will continue to use their legacy system as the system of record for the US Air Force's execution of foreign military training until that capability can be fully included in DSAMS in the future but the US Air Force will maintain certain reference data in DSAMS for use by SCOs, IMSOs, and the other MILDEPs.

C13.2.2. <u>DSAMS Management.</u>   The DSAMS Program Management Office (PMO) in DSCA (Information Technology Directorate) manages DSAMS. The IT Governance Board via the IT CRB approves any changes to DSAMS except for repair/maintenance under $500K. The Defense Security Assistance Development Center (DSADC), Mechanicsburg, PA, maintains the application. Additional information on DSAMS is available on the DSAMS web site at https://dsams.dsca.mil from the DSAMS PMO.

C13.2.3. <u>DSAMS Training.</u>   Implementing Agencies are responsible for DSAMS user training. The DSAMS PMO provides initial training support to key Implementing Agency personnel when new software releases change existing functionality or add new functionality. In addition, the DSAMS PMO provides training support and business process consulting support as resources permit. Implementing Agencies needing training or consulting assistance should contact the PMO at DSCA.

C13.3. <u>DSCA 1200 SYSTEM</u>

C13.3.1. <u>DSCA 1200 System Business Function.</u>   The DSCA 1200 System is a classified DoD system that contains a compilation of country data providing status of Foreign Military Sales (FMS) negotiations from LOR to closure/completion.

C13.3.2. <u>DSCA 1200 System Data.</u> The DSCA 1200 System contains two types of data records - case level records and item detail records. These data are input to the system by designated users using specific formats. Transaction types S1 through S7 are used to update case level records. Case transactions received prior to 4:00 PM (1600) are processed in the DSCA 1200 System update each night. The Defense Finance and Accounting Service, Indianapolis (DFAS Indianapolis) provides item detail data (reflecting delivery status) to DSCA by the close of business of the last working day of each month. This data is the "end of month position" from the previous month.

C13.3.3. <u>DSCA 1200 System Management.</u> The DSCA 1200 System is managed and maintained by DSCA (Information Technology Directorate).

C13.3.4. <u>DSCA 1200 System Reports.</u> Requests for DSCA 1200 reports should be sent to DSCA (Business Operations Directorate). Data is provided only on a need-to-know basis (i.e., Combatant Commands receive data for their area of concern, a Security Cooperation Organization (SCO) receives data only for its country, etc.). Many reports from the DSCA 1200 System are classified. Reports containing classified information (e.g., LOAs) are appropriately labeled.

C13.4. <u>DSCA 1000 SYSTEM</u>

C13.4.1. <u>DSCA 1000 System Business Function.</u> The DSCA 1000 System is an unclassified system that supports the Military Assistance Program (MAP), Drawdowns, and International Military Education and Training (IMET) program deliveries.

C13.4.2. <u>DSCA 1000 System Data Input.</u> Drawdown data are created by the MILDEPs and submitted to DSCA for entry into the DSCA 1000 System.

C13.4.3. <u>DSCA 1000 System Management.</u> The DSCA 1000 System is managed and maintained by DSCA (Information Technology Directorate).

C13.4.4. <u>DSCA 1000 System Reports.</u> Requests for DSCA 1000 reports should be sent to DSCA (Business Operations Directorate) and should identify how the requester would like the data sorted. Data are provided only on a need-to-know basis (i.e., Combatant Commands receive data for their area of concern, an SCO receives data only for its country, etc.).

C13.5. <u>DSCA FOREIGN MILITARY FINANCING (FMF) SYSTEM</u>

C13.5.1. <u>DSCA FMF System Business Function.</u> The DSCA FMF System is an unclassified system designed to administer FMF repayable and non-repayable loans, FMF grants and the MAP Merger program. The system includes five major functions:

C13.5.1.1. <u>Recording FMF Programs.</u> All apportionments of FMF funds, with the exception of administrative funding, are recorded in the FMF System.

C13.5.1.2. <u>Commitments.</u> FMF funding is used to finance FMS cases and, as allowed, direct commercial contracts. All uses of FMF funding are recorded as commitments of the original program value authorized, as a control to prevent overuse of funds.

C13.5.1.3. <u>Billing and Collecting.</u> Some FMF programs are in the form of repayable loans. The FMF System produces bills and credits repayments against repayable loans. The System also tracks repayment of DoD-guaranteed FMF loans and defaults.

C13.5.1.4. <u>Rescheduling, Refinancing and Debt Forgiveness.</u> Borrowers who are unable to honor original FMF debt repayment schedules frequently request the Paris Club for debt rescheduling and/or forgiveness. The USG is a member of the Paris Club and participates in numerous debt reschedulings and/or forgiveness. The FMF System includes procedures for these actions.

C13.5.1.5. Washington Headquarters Services (WHS) Accounting Transactions. The FMF System creates execution files that, when downloaded to the WHS Accounting module, create accounting records for the FMF program.

C13.5.2. DSCA FMF System Input Transactions. Users update the DSCA FMF System on a weekly basis. Commitments are entered via the Commitment Sub-System. Each update includes data sharing (output and input) with the Defense Integrated Financial System (DIFS). Case status, implementation dates, case descriptions, and collection data are fed from DIFS. Case commitments are provided to DIFS. The system copies and reformats user input of an accounting nature to the WHS Interface File. These transactions are then downloaded and transferred to the WHS Accounting System, which is the DSCA General Ledger for the FMF program.

C13.5.3. DSCA FMF System Management. DSCA (Business Operations Directorate) has management responsibility for the DSCA FMF System. The system is maintained and operated by DSCA (Information Technology Directorate).

C13.5.4. DSCA FMF System Reports. The DSCA FMF System has 34 active hard copy reports available. These reports provide a variety of FMF data for cases and direct commercial contracts financed with FMF funds, as well as loan, grant, and MAP Merger programs.

C13.6. MILITARY ARTICLES AND SERVICES LIST (MASL)

The MASL identifies defense articles and services and is a required entry on each LOA line item. There are two separate MASLs - one for materiel and one for training.

C13.6.1. Materiel MASL. DSCA (Business Operations Directorate) maintains the materiel MASL using the DSCA 1200 System and DSAMS. Each Implementing Agency should submit proposed additions, changes, and deletions to DSCA. The MASL contains the following elements.

C13.6.1.1. Generic Code. Each item listed on the MASL is assigned a generic code. The generic codes assigned to the defense articles and defense services are contained in Appendix 4.

C13.6.1.2. Federal Supply Classification (FSC). Each MASL line identifies the FSC. The FSC is a DoD code used to classify materiel, identified under the Federal Cataloging Program. The FSC contains four digits. The first two digits identify the Federal Supply Group (FSG) and the last two digits identify the Federal Supply Class within each group.

C13.6.1.3. National Stock Number (NSN). The NSN for an item consists of the applicable four-digit FSC, two-digit NCB Code, and a seven-digit National Item Identification Number (NIIN). All major items of materiel (except ammunition) listed in the MASL are identified by a specific NSN where one has been assigned by Defense Logistics Information Service (DLIS). Major items are assigned the proper FSC and a pseudo NIIN by the responsible MILDEP when an NSN has not been assigned as in the case of ships and aircraft.

C13.6.1.4. <u>"Major Items" Versus "Dollar Value" Lines.</u> The materiel MASL identifies whether a line is a major item or a dollar value line. Major items (e.g., aircraft) are identified in the MASL with a unit of issue other than "XX." Dollar value lines are groupings of related items (e.g., spare parts). Appendix 4 shows, by Generic Code, which items should be considered major items.

C13.6.1.5. <u>Footnote Code.</u> MILDEPs are responsible for the assignment of footnote codes, where applicable, to all lines under their cognizance. Footnote Code "NN" is assigned to items that are not available from supply, under normal circumstances, to meet requirements. If a replacement item is known, the new MASL data should be submitted to DSCA by the appropriate MILDEP. Dollar lines are not assigned this footnote code. Footnote Code "YY" is assigned to items that were previously available and used on an FMS case, but are now inactive.

C13.6.2. <u>Training MASL.</u> Air Force Security Assistance Training (AFSAT) Squadron (Training Operations) maintains the Air Force training MASL; Naval Education and Training Security Assistance Field Activity (NETSAFA) maintains the Navy MASL; and Security Assistance Training Field Activity (SATFA) maintains the Army MASL. The training MASL contains the following elements.

C13.6.2.1. <u>Generic Code.</u> Each item listed on the MASL is assigned a generic code. The generic code is used to classify training according to the budget activity for reporting and management purposes. A complete list of codes is shown in Appendix 4.

C13.6.2.2. <u>Execution Agency Code.</u> This is a three-digit code used with all training program lines to identify the MILDEP providing the training, the funding command or agency, and the school or training activity at which training is to be performed. The MILDEPS are responsible for assigning these codes (coordinated with DSCA (Programs Directorate)).

C13.6.2.3. <u>Training Analysis Code.</u> Used in management of the IMET program to group training program data by categories that facilitates analysis by overall IMET program objectives. See available codes in Chapter 10, Table C10.T4.

C13.7. <u>SECURITY ASSISTANCE NETWORK (SAN)</u>

C13.7.1. <u>SAN Business Function.</u> The SAN is an Internet-based system used by SCOs, International Military Student Officers (IMSOs), international purchasers, and other members of the DoD Security Assistance community worldwide.

C13.7.1.1. <u>SAN Objectives.</u> The objectives of the SAN include:

C13.7.1.1.1. To provide ready and simplified inquiry access to Security Assistance training management, case management, logistics management, financial management and, where applicable, international defense cooperation management information.

C13.7.1.1.2. To provide Combatant Commands, SCOs, IMSOs, international purchasers and other users with local software packages that can collate Security Assistance data, produce management reports, and generate computer-produced forms and formats.

C13.7.1.1.3. To provide electronic mail (E-mail) capability among Combatant Commands, SCOs, continental U.S. (CONUS) organizations, and other Security Assistance overseas activities that do not have ".mil" e-mail addresses. Additionally, to provide e-mail forwarding for those who do have ".mil" e-mail addresses and an e-mail capability for Security Assistance users on temporary duty.

C13.7.1.1.4. To develop the necessary systems to support a consolidated view of data where this view is identified as a necessary requirement or is in the best interest of the Security Assistance community.

C13.7.1.2. <u>SAN Components.</u> The SAN includes the SAN Web, the International SAN (ISAN), the IMSO Web, the Training Management System (TMS), and the Security Assistance Automated Resource Management Suite (SAARMS). Table C13.T1. describes the functions of each of these components.

Table C13.T2. Security Assistance Network (SAN) Components

SAN Component	Description
SAN Web	Supports Security Assistance users worldwide. Accessible through the Internet. Provides registered users with access to Security Assistance community databases including the Integrated Standardized Training List (ISTL).
International SAN (ISAN)	Similar to the SAN Web designed for international purchasers.
International Military Student Office (IMSO) Web and Security Assistance Office (SAO) Web	Tailored to the needs of the IMSO and SCO. Provides access to the same training data used by the Security Assistance Training Community.
Training Management System (TMS)	Desktop-based system. Provides Security Assistance training management functions to SCOs, Military Services, DSCA, and international purchasers.
Security Assistance Automated Resource Management Suite (SAARMS)	Provides resource management functions for SCOs, Combatant Commands, and other Security Assistance activities.

C13.7.2. SAN Management. Table C13.T2. shows responsibilities for SAN management.

Table C13.T3. Security Assistance Network (SAN) Management Responsibilities

Organization	Responsibility
DSCA (Information Technology Directorate)	Overall systems coordinator for the SAN Establish short and long-term goals and applications relative to the SAN. Provide funding for the SAN. Set technical standards for future computer and data accessory equipment purchases on behalf of SCOs. Review annual budget priorities relative to computer equipment purchases, maintenance arrangements, and telecommunications networks funded by DSCA. Maintain liaison with the Chairman of the Joint Chiefs of Staff, Combatant Commands, MILDEPs, and defense agencies to establish standard approaches and procedures to security assistance data accessibility.
DSCA (Programs Directorate)	Chair TMS, IMSO Web, and SAO Web Configuration Control Board (CCB).
DSCA (Business Operations Directorate)	Chair SAARMS CCB.
Defense Institute of Security Assistance Management (DISAM)	Manages and maintains the SAN under the oversight of DSCA (Information Technology Directorate). Manages system administration of the SAN systems and ensures compliance with DoD security and other computer system management requirements. Coordinates appropriate user account administration with the MILDEPs and Combatant Commands. Develops and supports TMS and SAARMS desktop software programs. Publishes and distributes the SAN user's handbooks. Provides initial training to DISAM students and follow-on training. Coordinates the central design and distribution of SAN packages for SCOs. Receives all proposed SAN changes and submits recommended changes through the SAARMS, TMS, or IT CRB as appropriate.
DFAS Indianapolis	Interface with the MILDEPs and defense agencies on database connectivity issues. Distribute disks containing current security assistance training program information to off-line SCOs.
MILDEPs	Respond to requests for technical and management assistance from the DSCA (Information Technology Directorate). Coordinate all changes to security assistance information systems, which might have an impact on SAN users through the respective Program Managers. Establish procedures to ensure data transmission validity and make pertinent databases accessible to authorized users.

Organization	Responsibility
	Assign SAN User Administrators. Submit proposed SAN changes to DISAM.
Combatant Commands	Assign SAN User Administrators. Plan, coordinate, and provide technical support for standardizing purchases, improving management, ensuring interoperability, and recommending/approving purchase and distribution of Automated Data Processing (ADP) equipment and software systems to support the SAN. Ensure that SCOs adhere to hardware and software standards established by the DSCA (Information Technology Directorate) and validate requirements for future ADP purchases. Supervise, direct training, and provide technical support to the SAN installed at the Combatant Command headquarters, components, and SCOs throughout the theater. Evaluate SAN operations as part of the Combatant Command inspections/staff assistance visits. Submit proposed SAN changes to DISAM.
SAN Users	Ensure that future ADP purchases adhere to the minimum specifications on the DSCA web site or request a waiver from DSCA (Information Technology Directorate) through the Combatant Command. Ensure appropriate user accounts and passwords are obtained and safeguarded. Submit proposed SAN changes to DISAM.

C13.7.3. <u>Training Management System (TMS), International Military Student Office (IMSO) Web, and Security Assistance Office (SAO) Web Configuration Control Board (CCB).</u> The TMS, IMSO Web, SAO Web CCB prioritizes TMS, IMSO Web, SAO Web and related SAN workload, makes resource recommendations to the DSCA (Business Operations). Members of the TMS, IMSO Web, SAO Web CCB include DSCA (Programs Directorate) (chair), DSCA (Information Technology Directorate), Combatant Commands, and DISAM. The IT Governance Board via the IT CRB approves all IT system enhancements to TMS, IMSO Web, and SAO Web except for repair/maintenance requests under $500K.

C13.7.4. <u>Security Assistance Automated Resource Management Suite (SAARMS) Configuration Control Board (CCB).</u> The SAARMS CCB prioritizes SAARMS and related SAN workload, makes resource recommendations to the DSCA (Business Operations Directorate. Members of the SAARMS CCB include DSCA (Business Operations Directorate) (chair), DSCA (Information Technology Directorate), Combatant Commands, DISAM, and DFAS. The IT Governance Board via the IT CRB approves all IT system enhancements to SAARMS except for repair/maintenance requests under $500K.

C13.7.5. <u>SAN Equipment.</u> The DSCA Web site under the section entitled "Equipment Purchases and Maintenance" shows the minimum equipment required to use the SAN. Any deviation from these specifications must be coordinated through the MILDEP, Combatant Command, and the DSCA (Information Technology Directorate). Moreover, all SCO ADP purchases must be coordinated with in-country embassy and/or mission representatives to ensure compatibility with the DoS security and maintenance standards.

C13.7.6. <u>SAN Training.</u> Newly designated Security Assistance personnel shall receive initial SAN Web familiarization training at DISAM. DISAM prepares, maintains, and distributes the SAN Web User's Handbook, which compiles system descriptions, security procedures, and product formats. The Combatant Commands, MILDEPs, and DISAM conduct SAN refresher and/or update training.

C13.8. <u>SECURITY COOPERATION INFORMATION PORTAL (SCIP)</u>

C13.8.1. <u>Security Cooperation Information Portal (SCIP) Business Function.</u> The SCIP is managed, administered, and maintained by DSCA (Information Technology Directorate). The SCIP allows security cooperation personnel, including our international partners, to have a tri-Service view of selected foreign military sales case-related data. The SCIP draws information from the MILDEP Security Assistance legacy systems and is provided to authorized users in a web-based, user-friendly, standardized tool. Users are granted access on a need-to-know basis as determined by their parent organizations (for USG users) or their Government's designated representative (for foreign purchasers). The IT Governance Board via the IT CRB approves all IT system enhancements to SCIP except for repair/maintenance requests under $500K.

C13.9. <u>CASE EXECUTION MANAGEMENT INFORMATION SYSTEM (CEMIS)</u>

By memorandum dated January 10, 2001, DSCA initiated a Case Execution Requirements Definition process, to analyze the deficiencies of existing Military Department (MILDEP)-unique case execution legacy systems. The analysis determined that there were sufficient deficiencies in these systems to warrant development of a Mission Needs Statement (MNS). A MNS was developed and approved on May 30, 2001 for a new system called CEMIS. CEMIS functions include post case implementation through case closure. A CEMIS high-level Operational Requirements Document (ORD) was approved in December 2001 and a more detailed ORD was produced in January 2003. These documents outline the functional and system requirements for the entire Security Assistance community to include international purchasers. Once the system has been developed, this Manual shall be updated to provide additional information.