



DEFENSE SECURITY COOPERATION AGENCY

WASHINGTON, DC 20301-2800

APR 16 2004

MEMORANDUM FOR DIRECTOR, DEFENSE LOGISTICS MANAGEMENT STANDARDS
OFFICE (DLMSO)

SUBJECT: Migration to the Defense Logistics Management Standards (DLMS) and Elimination
of the Military Standard Systems (MILS)

Reference: DLMSO memorandum, January 5, 2004, subject as above

In response to subject memorandum, attached is DSCA's final migration plan outlining the
background and schedule for the Case Execution Management Information System (CEMIS).

As DSCA briefed during the Unique Identification (UID) and DLMS Migration Workshop, 9-10
March 2004, CEMIS will be the Security Assistance community's tool for transitioning from
MILS to DLMS, and will ensure compliance with the Under Secretary of Defense (Acquisition,
Technology and Logistics) memorandum of December 22, 2003, subject as above.

The DSCA points of contact are Ms. Kathy Robinson, DSCA/P2, 703-601-4368, e-mail:
kathy.robinson@dsca.mil, and Mr. Tom Sippel, DSCA/IT, 717-605 9295, e-mail:
tom.sippel@dsadc.dsca.mil.

A handwritten signature in cursive script, reading "Freda J. Lodge".

Freda J. Lodge
Director
Policy, Plans and Programs

Attachment
As Stated

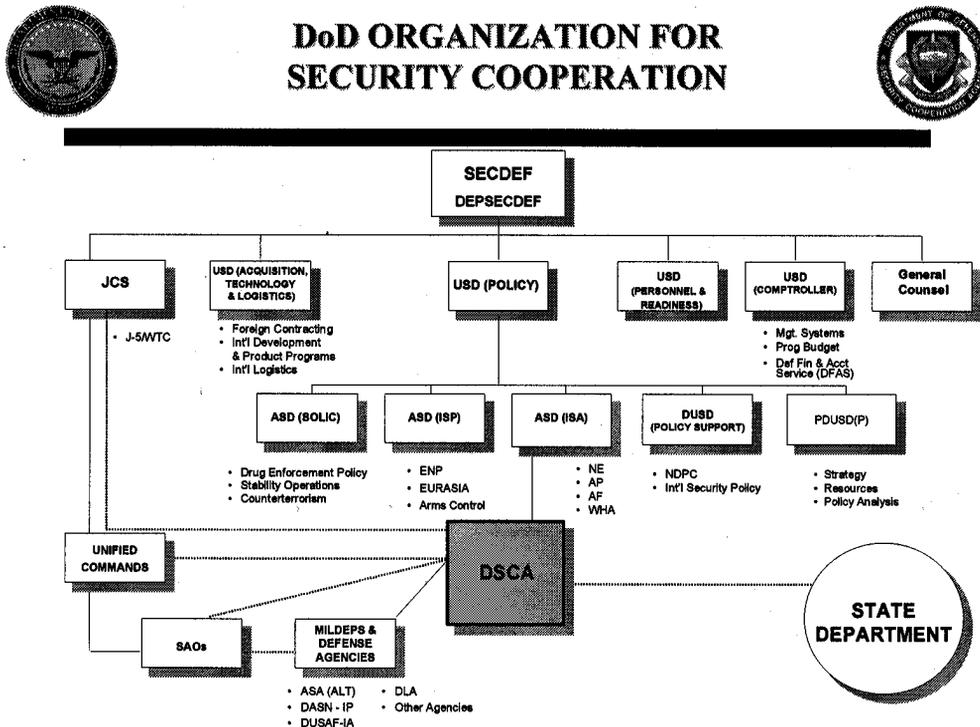
**DEFENSE SECURITY COOPERATION AGENCY
IMPLEMENTATION PLAN
16 APRIL 2004**

INTRODUCTION

Security Assistance is a group of programs, authorized by law, that allows the transfer of military articles and services to friendly foreign Governments. Security Assistance transfers may be carried out via sales, grants, leases, or loans, and are authorized under the premise that if these transfers are essential to the security and economic well-being of allied Governments and international organizations, they are equally important to the security and economic interests of the United States (U.S.). Security Assistance programs support U.S. national security and foreign policy objectives.

ORGANIZATION

The Defense Security Cooperation Agency (DSCA) is a separate agency within the Department of Defense (DoD) under the direction, authority, and control of the Under Secretary of Defense for Policy.



DSCA directs, administers, and supervises the execution (to include closure) of all Security Assistance programs for the DoD. DSCA is the DoD focal point for Government-to-Government arms transfers, budget, legislative, projections, forecasting, and other Security Assistance matters. DSCA conducts international logistics and sales negotiations with foreign allies, provides financial management, develops and

implements Security Assistance policy, and assists U.S. industry in exporting military equipment and services.

RESPONSIBILITIES

While DSCA is the DoD focal point for Security Assistance, the Military Departments (MILDEPs) execute the programs. Case execution is the core phase of the Foreign Military Sales (FMS) business, and is critical to the mission of DSCA. It includes detailed logistics and financial business processes to support the execution of cases - the ordering and delivery of the defense article or service to the international customer, and the accompanying payment.

A Case Manager at the MILDEP is responsible for the logistics and financial condition of the case. A Case Manager's charter is to ensure the customer's requirement is delivered as ordered, in a timely manner, within the Letter of Offer and Acceptance (LOA) value and certify the case for closure within a "reasonable" period of time. Standard case execution functions performed during this process include, but are not limited to, planning and organizing the execution tasks, directing appropriate funding, tracking funds distribution, and managing subsequent order processing, fulfillment, delivery reporting, case payment/disbursement, and closure.

LEGACY SYSTEMS

The existing case execution information systems used by the MILDEPs are aging, expensive to maintain, and fail to meet many of the current user requirements. These requirements include providing timely and accurate tri-service multi-country information not only to various offices within the Department of Defense, the Department of State, and Congress for key decision-making, but also to the Security Assistance leaders for more effective management in support of the Security Assistance mission. The requirements also include providing international customer satisfaction in an increasingly complex global environment. All of these systems use the Military Standard Systems (MILS) such as MILSTRIP, MILSBILLS, MILSTRAP or a combination thereof.

The current unclassified case execution information systems (independent single service systems) are:

- ✓ The Centralized Integrated System for International Logistics (CISIL) – Army (Developed in 1976)
- ✓ The Management Information System for International Logistics (MISIL) – Navy (Developed in 1989)
- ✓ The Security Assistance Management Information System (SAMIS) - Air Force (Developed in 1983)
- ✓ The Case Management Control System (CMCS) - Air Force (Developed in 1989)

In addition, there are other Security Assistance “satellite” systems involved in case execution. These systems augment the technology available in the legacy systems by adding a web-based capability, the ability to order and/or repair nonstandard parts for FMS customers, and other special services.

They are as follows:

Simplified Nonstandard Item Acquisition Program (SNAP)
Parts & Repair Ordering System II (PROS II)
Air Force Security Assistance Center (AFSAC) On-Line
Navy E-Business Suite
Supply Tracking And Reparable Return/Personal Computer (STARR/PC)*

*STARR/PC was designed using both MILSTRIP and “MILSTRIP-like” (e.g., XD_) transactions that need to be mapped in the Defense Logistics Management Standards (DLMS). STARR/PC is a PC-based system for FMS customers to use for requisition and Supply Discrepancy Reporting inputs and processing, and also contains freight tracking capability.

These systems are all funded by foreign government funds versus U.S. Government resources. Initially they were destined to be replaced by the continuation of the development of the Defense Security Assistance Management System (DSAMS), which is the system used throughout the community to prepare and implement Foreign Military Sales (FMS) Letters of Offer and Acceptance. However, in October 2000, DSCA cancelled further development of DSAMS for case execution, thus requiring the MILDEPs to continue using their existing legacy systems until an alternate plan was established.

The legacy systems suffer from the classical problem of being unique, outdated, and not capable of combining data into a single source of information. Currently, each MILDEP relies on separate systems and internal data that are tailored specifically for its specific case execution needs and in most cases are not compatible or interoperable with the processes used by another MILDEP. Legacy Security Assistance case execution systems require improvements to support the Security Assistance Program Manager, Case Manager, Executive level oversight, and international customer needs. There is a lack of DoD-wide standardized case execution processes, standardized data, accessibility to a shared database, and provision of a total country (tri-service) view. They do not adhere to DoD technical architectures and standards that are mandated by the DoD Technical Architecture Framework for Information Management. Also, they do not take advantage of modern, commercially available technology and have become very difficult and costly to maintain. In particular, most of the case execution systems reside on hardware and use software developed with 1970s –1980s development techniques and languages, and lack adequate system documentation. These limitations will become progressively more constraining and costly over time. For these reasons, the legacy systems are being replaced and will not migrate to the new DLMS.

A NEW DIRECTION

In January 2001 DSCA outlined a new effort known as the Case Execution Management Information System (CEMIS), the development of which followed a disciplined formal acquisition process in accordance with the DoD Directive 5000.1 and DoD Instruction 5000.2. Throughout FY 02 requirements teams gathered on a regular basis, with representatives from the MILDEP FMS community whose expertise covered all facets of case execution: logistics, acquisition, financial, systems development, and overall corporate knowledge. The teams identified requirements for CEMIS ranging from those that currently exist and should be retained for CEMIS, to new requirements needed to improve and enhance service to our international customers, as well as meet the increased demands brought about by the continuously-evolving automation needs throughout the world. One of the first requirements identified was the need for CEMIS to be built in accordance with the latest data exchange standards. This was also required to be in compliance with DoD Directive 8190.1 that mandated no new systems would be built in the MILS. Additionally, the new requirements could never be satisfied within the confines of the 80-character MILS format.

Concurrent with CEMIS requirements development, the Security Assistance community was also gathering data to design a system that would be a "short-term" solution prior to CEMIS deployment, given CEMIS' timeline. This system became known as the Security Cooperation Information Portal (SCIP), drawing in and consolidating data from the aforementioned legacy systems plus DSAMS. Since SCIP uses current legacy system data, SCIP is also built in MILS. The MILDEP websites will eventually be collapsed into SCIP. Once CEMIS achieves DLMS compliance, SCIP will also convert to DLMS.

THE CEMIS SOLUTION

After the teams completed the requirements identification process at the "20,000 foot level", an analysis of alternatives was conducted to determine the best way to meet the requirements that the teams had developed. After a thorough analysis of six different alternatives, DSCA chose the "Re-Host and Modernize" option.

The CEMIS Re-host effort translates/converts existing code and functionalities from the DSCA portfolio of legacy case execution systems into a single case execution system, utilizing a single Oracle database and operating on a modern platform with modern language(s). This methodology, distilled from six alternatives studied in the CEMIS Analysis of Alternatives (AoA), preserves the existing business rules while positioning the Security Assistance community for future enhancements, to include the migration to the Defense Logistics Management Standards (DLMS). The single system, CEMIS, is envisioned as a business management information system for planning, organizing, directing, and controlling Security Assistance Case Execution. The system will integrate case execution business practices with domestic acquisition, logistics, and financial infrastructures, and will provide program status and information to the Security Assistance global community. CEMIS will facilitate the transition of the legacy Security Assistance systems to a single data-managed database system using standardized

processes and shared data to accommodate a total community profile. CEMIS compliance will overcome the legacy systems limitations, and will optimize, streamline, and integrate the unique automated systems, subsystems, and databases into a single system for use across all three MILDEPs. It will improve the corporate decision-making process and end-user productivity through reduction of redundant databases, data transmission, and redundant tasks.

As an overview, the Re-host portion converts the current legacy systems from their existing languages and databases (shown below) into new, more modern, languages (Java or C++) and a “relational” database such as Oracle. Phase One of the Re-Host effort consists of a “4 to 4” simultaneous conversion of the legacy systems into the new language and database.

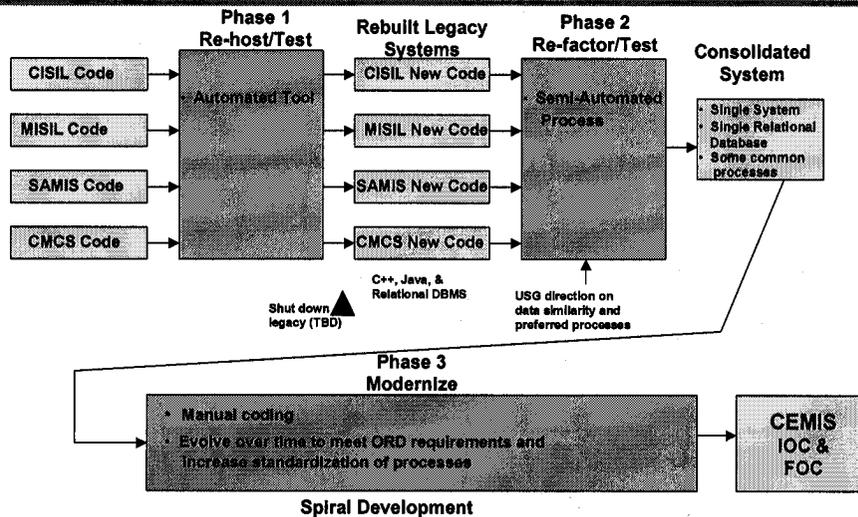
SERVICE	SYSTEM	LANGUAGES	SLOC	DATABASE	HDWARE
Air Force	SAMIS	Natural 1, ANSI COBOL 85	1.5M	ADATABASE	OS390/MVS
Air Force	CMCS	ANSI COBOL 85, JCL, FOCUS, REXX (MVS)	1.5M	FOCUS	VM
Army	CISIL	ANSI COBOL 85, JCL, M204	1.5M	Flat Files (VSAM, M204)	OS390/MVS
Navy	MISIL	ADSO, Assembler, ANSI COBOL 85	1.5M	IDMS	OS390/MVS

The source code will be translated from the four legacy case execution systems, containing multiple languages and different database, to four case execution systems using the same target programming language(s), database management system (i.e., Oracle) and operating in the same-targeted environment. **Target date to begin is FY 05.**

Once the source languages for the four legacy case execution systems have been successfully translated/converted to four systems with the same source language(s), database architecture and hardware platform, Phase Two begins. The four systems will be consolidated into a single case execution system. This consolidation phase will include refactoring (eliminating, replacing, and rewriting code) to improve the software architecture and design, code efficiency and maintainability. The result will be one fully integrated system that will be used by each MILDEP, thereby standardizing many of the processes each MILDEP uses for case execution. **Target date to begin is FY 06.**



The Re-host and Modernize 3-Step Strategy



TRANSITION TO DLMS

After successful completion of CEMIS Re-Host Phases One and Two, the Modernization effort will begin. It is during this phase that the DLMS ASC X12/XML migration will take place. One of the primary reasons for conducting the Re-Host project is to position us for the Modernization phase, and allow us to add the new capabilities identified during the CEMIS requirements determination phase. This is an extremely important body of work that will bring us into compliance with the DLMS mandate. By this time the individual MILDEP legacy systems will have been turned off and completely replaced by one integrated, standardized system. Other business functions will benefit from conforming to DLMS ASC X12/XML such as FMS transformation and business process reengineering initiatives, freight tracking capabilities, and end use monitoring requirements, to name just a few. Additionally, as the critical feeder system to MILDEP core accounting systems, CEMIS will include internal controls and financial reporting as specified in "A Guide to Federal Requirements for Financial Management Systems" that permits the Security Assistance community to be fully compliant with the statutory requirements of the Federal Financial Management Improvement Act (FFMIA) - which includes both the Federal Managers Financial Integrity Act (FMFIA) and Chief Financial Officer (CFO) Act. **Target date to begin is FY 07.**

TRAINING

As indicated above, CEMIS Re-host will take place in several phases before concluding in the phase known as "Modernization". Initially there will be minimal training of the CEMIS development staff in DLMS techniques and format usage. The Re-host process will not alter current business logic or processing code, and it is intended that all internal and external interfaces will remain as they are today. As a result, the need for a continued translation capability will continue until such time as CEMIS enters the Modernization phase, and interfaces are written in a DLMS-compliant format. Approximately one year prior to the beginning of the Modernization phase, CEMIS

developers will be properly trained in the development and use of DLMS formats, and will be made aware of existing translation code available within the DoD, predominantly at DAASC, to aid in writing new DLMS-based code.

TESTING

CEMIS testing will take place in accordance with a Test and Evaluation Master Plan (TEMP) currently under development specifically for the CEMIS project. Test transactions will be established for each condition, which cause the creation of DLMS transactions that will pass externally. Using traditional testing methods, the CEMIS development team will define transactions, establish the necessary pre-established conditions, and confirm individual test results.

FMS-UNIQUE ASPECTS

Security Assistance is a key policy tool for our national security objectives. It strengthens alliances and partnerships through close relationships with more than 180 customer countries and international organizations, having varying degrees of automation capability. Few, if any, international customers are currently using sophisticated X12 or XML transactions. The majority employs MILS-driven systems. While the more technically advanced customers will likely migrate to DLMS, and many are already transitioning to more sophisticated Enterprise Resource Planning systems, a great many will continue to use MILS for various reasons. Therefore, even when the U.S. systems migrate, communication with the international customer systems, regardless of the means of exchange used, must continue.

In order to do so, it is critical that translation capabilities continue between FMS countries and DoD organizations, either via the Defense Automated Addressing System Center (DAASC) or some other means. DSCA and the MILDEPs will encourage all international customers to transition to the new formats. In fact, over the past several years DSCA has already briefed several international customer groups on the reduced level of data they will receive if they choose to remain in MILS. However, in the end, it is the customers' decision to make.

SUMMARY

The Security Assistance Community welcomes the transition from MILS to DLMS for the numerous benefits and increased capabilities associated with the migration. It would be impossible to satisfy the new requirements identified for CEMIS using the MILS format.

After migration to DLMS, CEMIS will fully support DoD Security Assistance programs by incorporating standardized business processes and state-of-the-art data management tools to utilize resources more efficiently and effectively. It will incorporate flexible, state-of-the-art data management tools to accommodate changing business processes throughout the systems life cycle. Further, CEMIS will provide to the Security

Assistance community (to include international customers) greater visibility of, and access to, case execution performance information. It will be an integrated system that plans, organizes, directs, controls and measures the acquisition, delivery, and funding of FMS case material and services, and related Security Assistance programs.

The organization that will oversee this plan (point-of-contact, organization name and mailing address, phone and fax numbers, and email address):

Defense Security Cooperation Agency (DSCA)
1111 Jefferson Davis Hwy
Arlington, VA 22202

POCs:

Kathy Robinson (DSCA/Policy, Plans & Programs Directorate)

Phone: 703-601-4368/DSN 329

Fax: 703-604-6540 (DSN 664)

E-Mail: kathy.robinson@dscamail

Tom Sippel (DSCA/Information Technology Directorate)

Phone: 717-605-9295

Fax: 717-605-9315

E-Mail: tom.sippel@dsadc.dscamail