

1 SECURITY COOPERATION AUTOMATION

INTRODUCTION

This appendix provides an overview of some of the more common automation systems used by the security cooperation community. The overview includes the system description and functionality, as well as the procedures for requesting a user identification and password, if applicable.

SECURITY ASSISTANCE NETWORK

Background

In the 1990s, there was heightened interest in developing a more efficient way for overseas Security Cooperation Organizations (SCOs) and geographic combatant commands (GCC) to exchange information with the Department of Defense (DOD) and military department (MILDEP) security assistance management information systems and with individuals at all echelons within the security assistance community. Early in 1990, Defense Security Cooperation Agency (DSCA) formed a special task group to examine security assistance automation among prospective users. One of the objectives was to enhance the opportunity for access by GCC and SCOs, as well as continental United States (CONUS) based security assistance activities, to existing security assistance management information systems and to provide users labor-saving automated data processing (ADP) administrative tools. With this in mind, the director of DSCA established the following goals:

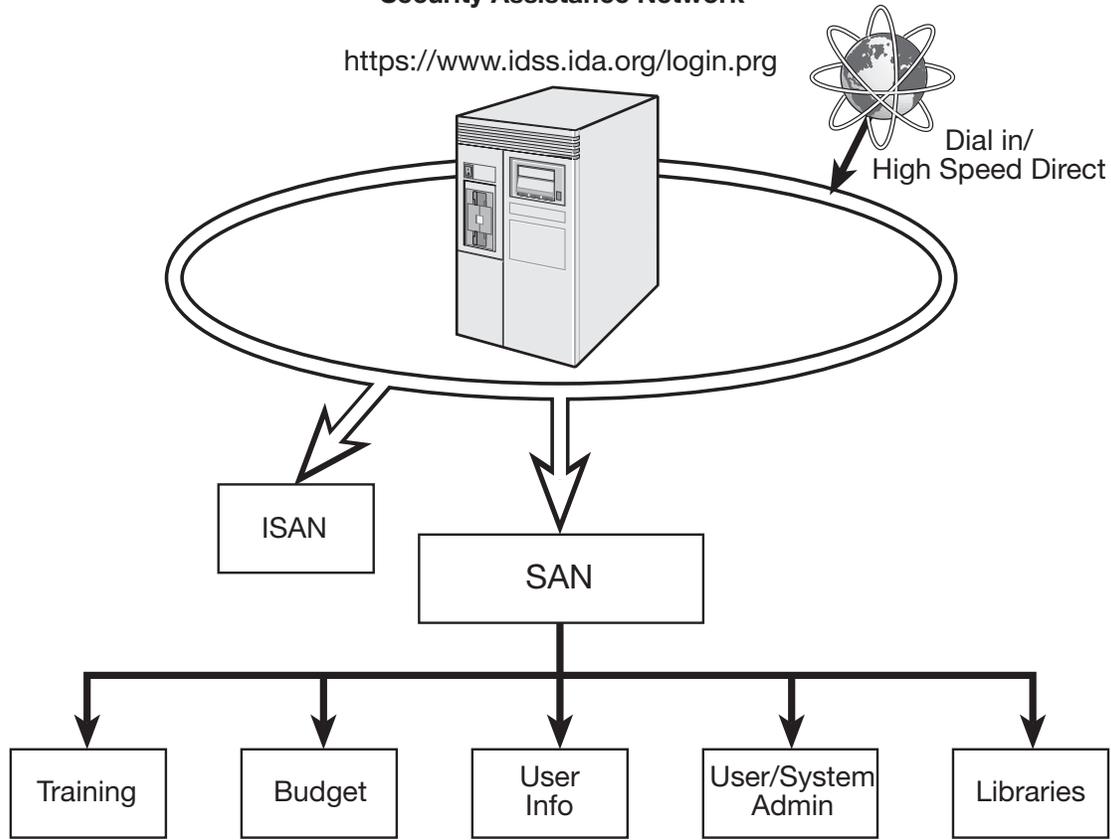
- Tie existing automated systems and users together
- Provide simplified access procedures to a range of automated systems
- Interface automated systems through existing or expanded telecommunications networks, providing automated communication and data exchange support

With the above objectives and goals outlined, the Security Assistance Network (SAN) was initiated, and is currently formalized in DOD 5105.38-M, *Security Assistance Management Manual (SAMM)*, chapter 13. The original telecommunications gateway for the SAN project was the Interoperability Decision Support System (IDSS), operated by the Institute for Defense Analysis (IDA). In the summer of 1996, development began on a web-based SAN. The concept of operations for the SAN web is quite simple. It is a web browser used to connect to the SAN home page via a local Internet service provider.

System Description

The SAN web contains many useful internal functions and links to many external systems operated independent of the SAN web. It must be noted that these are only links and the SAN web does not provide any connectivity to these systems. Therefore, if the user is restricted from accessing one of these external systems, logging into the SAN web first will not change this. Also, note that many of these external systems require a user identification and password. These user identifications and passwords are provided and managed by the system administrators for those systems. Figure A1-1 shows many of the internal functions and external links available to SAN web users. The SAN web can be accessed at: <https://www.idss.ida.org/san/login.prg>.

**Figure A1-1
Security Assistance Network**



User Database

Students attending the Defense Institute of Security Assistance Management (DISAM) Overseas Course (SCM-O) will automatically be registered as SAN users. Other requests for new SAN accounts can be accomplished by having an existing SAN user, acting as a sponsor, send a request electronically through the system. For detailed information on how to request a SAN account, please see the following webpage: <https://www.idss.ida.org/sanweb/How%20to%20Request%20a%20SAN%20Acct.doc>. Users can locate information about other SAN users by searching the user database. They can search by name, security assistance country code, organization, etc.

Library

Users can share files with other SAN users by uploading them into one of the libraries. Libraries can also be used to overcome smaller file size limitations of e-mail systems. Information in these libraries must be unclassified.

Budget

The budget section provides access to the Security Assistance Automated Resource Management Suite (SAARMS) and the Integrated Security Assistance Automated Resource Management Suite (ISAARMS). SAARMS will be discussed later in this appendix. ISAARMS is an electronic interface among the SCOs, the GCC, and the Defense Finance and Accounting Service (DFAS) and is only applicable for Security Assistance Administrative (T-20) funds. Twice a week, T-20 financial information is uploaded from SAARMS to ISAARMS for use by the GCCs and DFAS. GCCs and SCOs can find current and archived data on this site by country or command. DFAS uses this data to update their official accounting records. In return, DFAS produces a file of active financial documents, which is used to reconcile each country's financial records in SAARMS.

Training

The training section on the SAN provides the user with access to the various international military training databases such as the Training Military Articles and Services List (T-MASL) and the Standardized Training List (STL). SCO users can access this data for their individual countries. MILDEP and GCC users can access multiple countries. Data updates are on a daily basis for all of the military services.

TRAINING WEBS

The IMSOweb and the SCO-Tweb, discussed below, will eventually change names and both will be referred to as the “Training Management System, TMS.” Depending on the user's role, IMSO or SCO, different functions will be available once the TMS system is accessed. For now, the current names of IMSOweb and SCO-Tweb are used in this publication.

International Military Student Office Web

The IMSOweb is an Internet-based tool allowing the International Military Student Office/Officer (IMSO), at a training location to manage international military students (IMS) assigned to their schoolhouse. The IMSOweb is maintained on and receives its data from the SAN.

The IMSO web provides a means for the IMSO to identify international student quotas assigned to their training activity, receive arrival information on those students and report the student's progress as they advance through the training program. The IMSOweb also enables the IMSO to document detailed information about their location and schoolhouse which is available online for the training community.

Security Cooperation Office-Training Web

The SCO-Tweb is an Internet based tool allowing the SCO to manage their training program online. The SCO-Tweb is maintained on the SAN and receives STL and MASL updates from DSAMS.

In addition to allowing the SCO to view STL and training MASL information online, the SC-Tweb has several other very important features. The SCO-Tweb is where the SCO enters International Military Student information and creates Invitational Travel Orders (ITO) for the students. The SCO is also able to look up schoolhouse and IMSO information. The SCO can also maintain SCO POC information within the SCO-Tweb so that it is available to the training community. SCO-Tweb is required to be used for submission of student nomination packages for the Combating Terrorism Fellowship Program (CTFP). The other application that the SCO-Tweb is used for is the submission of the Combined Education and Training Program Plan (CETPP).

International Security Assistance Network Web

The International Security Assistance Network web (I-SANweb) is an Internet tool that provides essentially the same data accessibility to an international user from a host nation that is provided to US SCO users via the SAN. Thus, international users can access the training MASL data to identify desired courses of instruction. They can see course location information, and can have complete visibility of all country training programs that have been established for their country by viewing the STL. The I-SAN is a read only tool for the International customer. They cannot enter or change any information via the I-SAN. International customers who would like access to the I-SAN should contact their SCO in-country for further guidance. The SCO can then initiate a request for I-SANweb access for the international customer using the main menu of the SAN. The I-SANweb can be accessed at: <https://www.idss.ida.org/isan/login.prg>.

COMMERCIAL SECURITY ASSISTANCE NETWORK

The Commercial Security Assistance Network (C–SAN) is an Internet tool that provides contractors who have an active government contract or other DOD personnel access to the security assistance personnel roster worldwide. Contact DSCA at (703) 602-2015 to obtain a user identification and password for this For Official Use Only (FOUO) system. C–SAN can be accessed at: <https://www.idss.ida.org/csan/login.prg>.

FINANCIAL AND LOGISTICS DATABASES

Prior to discussing the financial and logistics databases maintained by DFAS, Army, Navy, and Air Force security assistance agencies, several key points should be noted. First, all access to these databases is read-only, unless special permissions are granted. Although it is recognized that personnel in the SCO and other communities need access to the data, only those personnel responsible for actions have write or change capability. Second, use of the SAN does not require access to or a full understanding of the total database. Thus, SCOs do not see the same screens as the CONUS action offices. Those elements and screens that were deemed necessary were modified and simplified to give the SCO a clear, concise picture of foreign military sales (FMS) case/line/requisition data. Finally, the data viewed is just a snapshot of what is occurring. After viewing, it is considered a historical record because within days, or perhaps hours, the data can change.

Defense Integrated Financial System

System Description

The Defense Integrated Financial System (DIFS), managed by Defense Finance and Accounting Service-Indianapolis Center (DFAS–IN) in Indianapolis, Indiana, is the integrated system for all security assistance financial data. Financial data from the FMS letter of offer and acceptance (LOA) through case closure is maintained by the DIFS system.

Functionality

Simplified screens have been developed for the SCOs providing required data in an easily readable form. For in-country SCOs, data is available for that country only. For GCC desk officers, data can be made available for all countries of responsibility. For standard DIFS system users the following data is available:

- Country implementing agency (IA) summary totals
- Financial status-country, and financial status-IA for country level data
- LOA detail summary and financial data
- Billing status data
- Payment schedules for LOA
- LOA line level data
- FMS case inventories
- Case controls
- Budget
- Case closure certificate inventory

- Performance/FMS Detail Delivery History Search Reports (FK)
- Cash
- Financial summary totals
- DIFS tables

Registration

To register for DIFS access the user must submit a completed DD Form 2875, System Authorization Access Request (SAAR), to DFAS. The basic form is available online: <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo3211.html>.

DFAS has developed a special continuation sheet that explains what is required in block 27 of the form. To request the continuation sheet and submit the completed form, email DFAS-IN-DIFS-ACCESS-REQUEST@DFAS.MIL or contact the administrator at:

DFAS-JAXDC/IN
 8899 E. 56th St.
 Indianapolis, IN 46249
 Fax: (317) 212-1917 (No DSN)
 Tel: (317) 212-0977/7396, DSN 699-0977

Management Information System for International Logistics

System Description

The Management Information System for International Logistics (MISIL) is the US Navy's logistics and financial tracking system for security assistance. MISIL has standardized screens for SCO use.

Functionality

Some of the most useful screens and uses are as follows:

- The case management screen depicts material provided, summary case information, and the name and phone number of the case manager.
- The case/amendment/modification screen provides implementation dates of the latest amendments/modifications and the number of any pending case actions.
- The case line summary screen provides a description and dollar value for every line on an LOA and identifies lines supplying major defense equipment (MDE).
- The case line detail screen provides data such as material supplied, source of supply, disbursements, obligations, for a specific case and line.
- The case financial screen provides financial data for each line of a case as well as case totals.
- The case management history screen shows chronologically the impacts on a case by amendments and modifications.
- The requisition screen provides detailed information on the current supply, shipment, and delivery status of any requisition for a given case.
- The supply discrepancy report (SDR) or report of discrepancy screen gives general and specific information on all SDRs submitted against a case.
- The FMS case listing report area enables the user to generate a complete listing of all cases for a specific country.

In addition to these simplified screens, the SCO also has access to selected MISIL screens which are used by CONUS FMS case managers.

Registration

To obtain access to MISIL, the user must submit a completed DD Form 2875, System Authorization Access Request (SAAR) and forward it to:

NAVSUP WSS-OF
ATTN: P7612
700 Robbins Avenue
Philadelphia PA 19111
Fax: (215) 697-0333. DSN 442-0333
Tel: (215) 697-2774, DSN 442-2774

Centralized Integrated System for International Logistics

System Description

The Centralized Integrated System for International Logistics (CISIL) is the Army's automated system used to support the management of security assistance programs. CISIL is the central repository for all Army security assistance and provides a series of databases which offer users of the system information needed to manage their specific program. The system is comprised of modules of data which interact within the system and also interface with other external sites/activities for exchange of information. The SCO menu within CISIL provides access to various levels of information to assist the SCOs in managing the programs under their area of responsibility.

Functionality

The CISIL SCO menu provides the user access to logistical and financial information at case, line and requisition levels specific to their programs. It also provides useful case management reports, case history, requisition and supply discrepancy report (SDR) data. One of the areas currently provided under CISIL SCO data is the case requisition review report sometimes referred to as the mini-audit report or case audit report. Although designed for US Army Security Assistance (USASAC) personnel, SCOs may find the open inhibitors option and the case requisition review option very helpful. Much of the same data in CISIL can be viewed in the user-friendly web-based Security Cooperation Information Portal (SCIP).

Registration

To obtain access to CISIL, the user must submit a completed DD Form 2875, System Authorization Access Request (SAAR) and forward it to:

USASAC-S
ATTN: Security Manager
54 M Avenue, Suite 1
New Cumberland, PA 17070-5096
(717) 770-4735 DSN: 771-4735
(717) 770-7052/7845; (DSN) 771-7052/7845

Security Assistance Management Information System

System Description

The Air Force Security Assistance Center (AFSAC) is responsible for administration of the security assistance program within the Air Force Materiel Command (AFMC). Security assistance program activities start with the initial negotiation of agreements for AFMC-managed initial and follow-on support cases, continue with the delivery of logistics support and end with the completion of all financial aspects of the programs for which AFMC is responsible. The Security Assistance Management Information System (SAMIS) is the Air Force's primary logistics information system for security assistance.

Functionality

The SAMIS maintains and reports comprehensive data on AFMC-managed security assistance programs. This information comes from many different sources; however, most data originates from various Air Force data systems. SAMIS serves as a repository for FMS case information, requisitions, supply status, shipments, and billing information required by AFSAC to effectively manage security assistance programs. SAMIS provides the security assistance community with accurate and timely information. To accomplish this, SAMIS provides on-line, real-time data updating as well as batch processing functions.

Registration

The SAMIS is a password protected system. A DD Form 2875, System Authorization Access Request (SAAR) is required for both US government (USG) (including SCOs) and international customers. Access to SAMIS can be requested via the AFSAC website at <https://afsac.wpafb.af.mil>, "Apply for AFSAC Online and/or SAMIS Account." Access to SAMIS and AFSAC online is granted based on a person's "need to know." Users are assigned specific permissions and privileges according to their FMS task requirements. Once the SAAR is approved, a user identification and password will be issued. There are four application formats based upon the category of the user:

- USG civilian and military—This category consists of AF, DOD, and other USG employees including those working in overseas locations such as SCOs.
- USG contractor—This category includes contractors employed by USG that need to access FMS data as approved by the command country manager and/or the system administrator.
- CONUS foreign national representatives and support contractors—This group includes foreign representatives and contractors employed directly by the country that work within the continental US (CONUS) such as freight forwarder employees, Foreign Liaison Office (FLO) employees, embassy personnel, and any US citizen employed by a foreign country.
- OCONUS foreign national representatives and support contractors—This category includes individuals listed in above that are located outside of CONUS (OCONUS). It is important to note that this category of user is required to forward their request for access through their embassy in Washington, DC.

DEFENSE SECURITY ASSISTANCE MANAGEMENT SYSTEM

System Description

The Defense Security Assistance Management System (DSAMS) is a DOD standard system operating under a modern information technology infrastructure encompassing the migration and reuse of selected features of existing security assistance systems. Incorporating an extensive analysis of the security assistance business area and its processes, DSAMS provides a set of standardized, improved,

streamlined, and optimized services. The major benefits of DSAMS are consolidated data, improved data quality, standard reports to the customer, faster building of cases, and a current implemented view when a case is opened in DSAMS.

Functionality

Case Development Module. The case development module (CDM) provides functionality from the entry of an initial request through the development of a FMS LOA and changes resulting in a modification or an amendment. The CDM also initializes centralized reference tables and workflow applications that are used in other modules. Enhancements over the past few years include additional functionality to enable electronic countersignature, and support for other security assistance programs such as leases.

Case Implementation Module. The case implementation module (CIM) covers the process from receipt of customer acceptance through issuance of implementing directions to the case manager and performing activity.

Training Module. The training module (TM) replaced the three MILDEP legacy training management systems, and includes automated interfaces with the SAN and TMS systems. This allows the automated upload of international student data into DSAMS, and automated the invitational travel order (ITO) funding process. DSAMS TM also allows the automated processing of cross-service training requirements across MILDEP channels.

Registration

DSAMS is a password protected system for use by USG personnel only. A DD Form 2875, System Authorization Access Request (SAAR) is required for access to DSAMS. Access to DSAMS applications is through the Citrix application only. Applicants for Citrix user accounts must email or fax a completed SAAR to the DSAMS help desk. The e-mail address is saar@dsadc.dsca.mil and the fax is DSN 430-9082. However, the user must have a valid DSAMS account, provided by a MILDEP, before a Citrix account is provided.

Once access is approved, a user identification and password for Citrix will be issued. The issuance of the DSAMS accounts is done through the appropriate MILDEP points of contact. Any additional questions should be directed to:

DSAMS Help Desk
helpdesk@dsadc.dsca.mil
717-605-9200; (DSN) 430-9200

DSAMS does not permit system access by international customers. There is a daily interface from DSAMS to the SCIP which provides FMS customers access to selected DSAMS data.

SECURITY COOPERATION INFORMATION PORTAL

System Description

The Security Cooperation Information Portal (SCIP) is a DOD-managed web-based (<https://www.sportal.us/home/>) system that provides access to FMS and security cooperation (i.e. Bulding Partner Capacity (BPC)/pseudo cases) case-related data extracts as well as numerous other capabilities. Since the SCIP system web address is a non-DOD domain, authorized users (i.e. with existing system accounts), can gain access from any (i.e. does not require .MIL) Internet connection. USG SCIP users typically use their USG DOD Common Access Card (CAC) to log-on. Foreign purchasers use their issued SCIP tokens to log-on to their SCIP account. Foreign purchaser's (and their designated freight forwarders) obtain their SCIP tokens from their country's designated Host Nation Token Administrator (HNTA) as a prerequisite to registering for a SCIP account. System accounts and access are available to both authorized USG (including non-DOD such as State Department, Coast Guard, etc.) users,

and foreign purchasers (including their designated freight forwarders). The data extracts come from multiple legacy MILDEP systems as well as other financial and logistic systems, including DSAMS and DIFS. Another major advantage of SCIP is that it is a tri-service (i.e. Army, Navy, Air Force) system that provides authorized users access to that MILDEP data via a single system account. Figure A1-2 displays the multiple data sources used by the SCIP system. To have access to all this data if SCIP did not exist, users would have to obtain (if authorized) separate individual accounts on each of those systems and have numerous user identifications and passwords. The SCIP system data is obtained by copying (i.e. snapshot vice real-time) the MILDEP and DOD system data as depicted in figure A1-2. Typically, the data is copied at least once a day. The latest update status, date, and time, is posted in the Case Information Community.

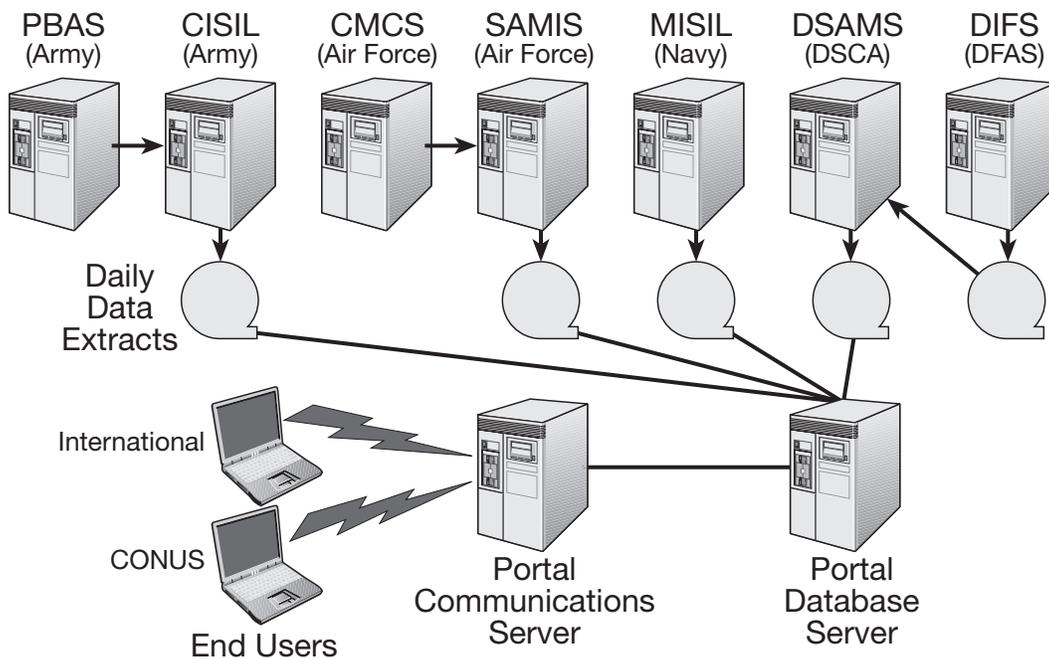
Functionality

SCIP system and data access permissions are set for various data levels ranging from all SCIP system data to single case view only. These access permissions are based on the user's system registration request and subsequent approvals according to user operational requirements and clearance. Data is separated by system tabs into different “communities.” A brief description of each SCIP community follows.

Home Community

The Home Community’s page is the first page users see when they successfully logon to SCIP. This community and other SCIP communities display announcements regarding both current and planned updates to SCIP information and releases.

**Figure A1-2
Security Cooperation Information Portal**



Case Information Community

The SCIP Case Information Community provides multiple features and capabilities to view, extract and input FMS and security cooperation (i.e. BPC/pseudo) case information. Menu options in this community include Case Status, Adhoc, Inputs, Information Extracts, Requisition Summary, and Financial Management Review (FMR) Case Sheets.

Case Status: Selecting that Case Information Community menu item provides a multiple-option filter/query capability to find, select, and view authorized FMS and security cooperation (i.e. BPC/pseudo) case information. Information from predetermined reports or from user-defined ad hoc queries is provided to the end user. A summary report can be printed or a Microsoft Excel file of the queried system data can be exported. The following types of “Case Status” information are available for all authorized FMS and security cooperation (i.e. “pseudo cases”) case versions (e.g. Basic, Modifications, and Amendments):

Case

- Provides a brief description of a case
- Case Information, Funding, Requisition Information, and Case Closure

Document

- Provides information on document types for a particular case regardless of whether they are implemented or in progress.
- Each tab is divided into five different sections: Document Information, Funding, Financial Data, Payment Schedule, and Quarterly Payments

Case Line

- Select an individual line from a case of interest to display the report with the following headings: Case Information, Requisition Information, Case Values, and Case Milestones.

Active Requisition

- Displays an active requisitions list of all open requisitions (shipped and unshipped) within the previous ninety days. If material on any requisition has been shipped, there will be a hyperlinked transportation control number (TCN). Clicking that TCN hyperlink will provide all available transportation details for that requisition shipment via the enhanced freight tracking system (EFTS) application.

Supply Discrepancy Report (SDR)

- Provided details on open or completed SDRs within the last year (at a minimum)

Document Timeline

- Provides a list of twenty selected milestones and dates from “cradle to grave” (e.g. customer request, offered, implemented, actual closure date, etc) which apply to that case or program.

Adhoc: A new adhoc report can be generated by selecting a report (Case-Level, Line-Level, Active Requisition, SDR, or Payment Schedule) or a saved adhoc can be run (names, if available, are listed in the user selectable dropdown menu).

Inputs: This Case Information Community menu item provides an authorized FMS purchaser user with the capability to input a variety of FMS Military Standard Requisitioning and Issue Procedures (MILSTRIP), and MILSTRIP-like transactions. Once entered, those transactions are partially validated in SCIP, and then relayed through the DLA Transaction Services to the appropriate MILDEP FMS case execution logistics computer system (MISIL, CISIL or SAMIS) for processing several times per day. The transactions, which can be created in SCIP, may be functionally grouped as follows:

- Requisitions
- Supply Discrepancy Reports
- Freight Tracking

Information Extracts: Authorized users can view all requisitions (i.e. active and historical) associated with a case, regardless of the current logistics or financial posture of those requisitions via the Information Extracts page. The process is performed overnight upon request as SCIP obtains information from the FMS case execution systems. Only one request is allowed per user per 24-hour period. After the overnight process is complete, resulting files are transmitted to SCIP and a notification on the Information Extract screen appears for the requesting user stating the extract data is available for download.

Requisition Summary: Various report options (e.g. Requisition Summary by Implementing Agency, Requisition Summary by Customer Service, and All Country Requisition Summary) which summarize requisition types, requisition numbers, and requisition amounts. The summary reports, however, do not provide any specific individual requisition's details about the summarized requisitions.

FMR Case Sheets: This is a DOD tri-service application. This page allows users to select cases for download and printing all FMR case sheets. Selection can be made by country; country and implementing agency; or country, implementing agency and case. Upon making a selection, links will appear below the selection criteria that, when clicked, will open an Excel file containing information specified with the selection criteria.

EUM Community

The End-Use Monitoring (EUM) Community provides specific information and capabilities to the authorized DSCA, SCO, and geographic combatant command (GCC) users to support the DOD (Golden Sentry) EUM program.

Case Execution Community

This community currently houses links to several tri-service applications, notably the Enhanced Freight Tracking System (EFTS) and FMS EMALL and Asset Visibility (AV) applications.

State Department Community

When implemented, the DOS Community will provide a means to automate the previously paper-bound process for requesting and tracking third party re-transfer requests and DOS approvals/disapprovals.

National Geospatial-Intelligence Community

The National Geospatial-Intelligence Community allows authorized SCIP users to access, review, and download aeronautical en route and approach charts, terminal procedures, etc. required for necessary international navigation and flight safety.

Security Cooperation Management Suite

The Security Cooperation Management Suite (SCMS) Common Operational Picture (COP) fuses SCIP data into numerous pre-formatted reports (e.g. Dashboard, Metrics, Reports, etc.) to authorized USG users to support their management and oversight of FMS cases and security cooperation (i.e. pseudo cases) programs. SCMS (COP) also is utilized for authorized USG personnel to enter inputs (see DSCA Memo 11-16, dated 09 May 2011, for additional details) for certain applicable security cooperation (i.e. BPC/pseudo cases) programs. This community is restricted to USG personnel only.

SCO/COCOM Community

This community is designed to be an information sharing type of community vice a business process or business application community, as are the other SCIP communities. It incorporates General Information and Lessons Learned–Best Practices intended for information and reference for the SCO/COCOM SCIP users. This community is restricted to USG personnel only.

Partner Info Community

This community is designed to be an information sharing type of community vice a business process or business application community, as are the other SCIP communities. It incorporates International Customer User Group (ICUG), Foreign Procurement Group (FPG), and various SCIP development team documents and artifacts, including, but not limited to:

- Agendas
- Meeting minutes
- Presentations

Corporate Info Community

This community is automatically available to all USG users of SCIP. It provides important information regarding security cooperation community metrics, Security Cooperation Business Forum (SCBF) and Performance Measurement Senior Working Group (PMSWG) meeting minutes and artifacts, Continuous Process Improvement (CPI), and Lean Six Sigma (LSS) initiative documents. It also now has a Lessons Learned–Best Practices section where applicable approved documents are categorized and uploaded for reference and information. Community users can also nominate new submissions to this section.

Navy Community

Web-based application programs that were previously available through the Navy E-Business application website are now available only through the SCIP Navy Community. All previous Navy-only applications, such as CEPT, the Navy’s FMS Information Warehouse WebRoR, etc. can be found under the SCIP Navy Community tab.

Help Community

This community provides SCIP users the option of electronically submitting a SCIP help desk trouble or issue input. Responses will be posted and filed by category (e.g. Pending, In-Progress, Complete, and Cancelled) for future reference and info by the submitting SCIP user.

Registration

The registration forms for both US and international users can be found by accessing the SCIP website and selecting the “Registration Information” button. International customers first require the use of a secure token to be issued by their designated Host Nation Token Administrator (HNTA). DSCA Memorandum 03-11, Enrollment Process for the Security Cooperation Information Portal, and DSCA 05-17, SCIP Electronic Token Issuance and Replacement Processes have all the details concerning issuance of tokens.

Additional memorandums on the use of SCIP can be found on the DSCA website at <http://www.dsca.mil/>. For additional assistance the user can contact:

Security Cooperation Information Portal (SCIP) Help
E-mail: sciphelp@dsadc.dsca.mil
SCIP Phone Support:
(717) 605-9200, DSN 430-9200

ADDITIONAL SOFTWARE PACKAGES

Security Assistance Automated Resource Management Suite

System Description

The Security Assistance Automated Resource Management Suite (SAARMS) is a group of one stand-alone and two web-based software applications used by SCOs and GCCs to manage their security assistance funded resources. The SAARMS applications are Budget Preparation, Budget Execution, and Property.

Functionality

Budget Preparation—This program standardizes the budget preparation process in a web-based format. It uses relevant historical data from previous budget submissions and periods of financial execution and generates the required budget submission reports that SCOs and GCCs are required to submit to DSCA during the budget submission cycle.

Budget Execution—This program is a web-based funds management feeder system that automates the record keeping of the SCO budget management functions. SAARMS feeds into the official DFAS BQ accounting system by conducting twice-weekly electronic transfers of data via the SAN.

Property—This program is a stand-alone application that is used for property book management, to include accounting for property and tracking property acquisition, use, and disposition.

International Training Management Website

The International Training Management (ITM) website is an informational website intended for all US and foreign international training managers. It provides a full range of international training management information, including references, policy and procedural messages, articles, lessons, exercises, FAQ sheets, links, and specific functional information.

The ITM website is available to anyone at <http://www.disam.dsca.mil/itm/> and does not require the use of a password.

DOD Acquisition Portal

System Description

The DOD Acquisition Portal is designed to be a single point of access to DOD acquisition related resources and information. This web-based system easily links users to the myriad of acquisition source documents, references, and other related information. The acquisition portal replaces its two predecessors, the Acquisition Knowledge Sharing System (AKSS) and the previous Defense Acquisition Deskbook (DAD) system.

Functionality

Acquisition Process—Covers the three primary acquisition processes of the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System (DAS), and the Planning, Programming, Budgeting and Execution (PPBE) system. This includes links to DOD and MILDEP policies, guidance, tools and other resources.

Workforce—Provides information on acquisition career management, the DOD human capital initiative, career planning, leadership training, and relevant professional organizations.

Policy—Serves as an encyclopedic source of acquisition policy that follows a hierarchy of policy issuance that can also be filtered by organization, career field and special topics.

Communities of Practice—Offers links to the various acquisition communities of practice and special interest areas.

Training and Continuous Learning—Outlines various training resources and continuous learning opportunities applicable to DOD acquisition professionals.

Industry—Functions as a one-stop source for information and links about industry partner support and participation in defense acquisition.

Workforce Support—The acquisition portal also provides a link to the DAU's "Ask a Professor" (AAP) program. AAP serves as a vehicle for practitioners within the DOD workforce to submit acquisition related questions that are routed to the appropriate subject matter expert for a response. AAP contains a user accessible Frequently Asked Question (FAQ) database that can be searched by key word or by category. FMS related questions are contained within the "International Foreign Military Sales" sub-category within the overall "Contracting" category.

Registration

The acquisition portal is hosted by the Defense Acquisition University (DAU) on behalf of the DOD acquisition community. You can access the acquisition portal at: <https://dap.dau.mil/Pages/Default.aspx>. The portal structure consists of a home page with general acquisition information and links.

SUMMARY

Security cooperation personnel have access to numerous automated systems, some that have been in existence since as early as 1976. Access has transformed from direct links for a few specific users to worldwide access via the Internet. Newer systems such as the SAN and SCIP have been specifically designed with the needs of the end-user in mind. Users in the far-flung corners of the security cooperation globe are freed from the constraints of time zone differences and slow mail delivery by virtue of Internet connectivity and interaction. Use of these systems has greatly enhanced communication between the SCO, GCCs, and CONUS-based logistics and training activities such as the MILDEPs and IMSOs and the international customers. The impact the increased access to the systems discussed in this annex has been profoundly beneficial, not only to security cooperation activities, but ultimately to the international customer as well.