Appendix A

Security Cooperation Automation Appendix

Introduction

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

Security Assistance Network

System Description

The Security Assistance Network (SAN) is a portal through which the Security Cooperation–Training Management System (SC-TMS) and the International Affairs Certification Program (IACP) can be accessed. The SAN is for use by Security Cooperation Offices (SCOs), Combatant Commands (CCMDs), MILDEPs, DSCA, DFAS, DOD schoolhouses, Regional Centers (RCs), and other organizations involved in security cooperation.

The International-SAN (I-SAN) is a portal through which international host nation organizations can access the Partner Security Cooperation-Training Management System (PSC-TMS) discussed below.

Registration

Students attending the Defense Security Cooperation University (DSCU) 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 web page: https://dscu.edu/documents/scwd_d/gaining_access_to_scwd_d.pdf.

Training Management on SAN

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) via the Security Cooperation-Training Management System. SCO users can access this data for their individual countries. MILDEP and CCMD users can access data for multiple countries. Data updates are performed on a daily basis for all of the military services.

Depending on the user's role, International Military Student Office (IMSO) or SCO, different functions will be available to the user when logging into SC-TMS via the SAN.

SC-TMS for the International Military Student Office

Based on the IMSO role type, various functions are available within SC-TMS for use by IMSOs to manage international military students (IMS) assigned to their schoolhouse.

SC-TMS for IMSOs 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. SC-TMS also enables the IMSO to document detailed information about their location, schoolhouse, and point of contact information, which will then be available online for the training community.

SC-TMS for the Security Cooperation Office

Based on the SCO role type, various functions are available within SC-TMS for use by SCOs to manage their country's SC international military training program. In addition to allowing the SCO to view STL and T-MASL information online, the SC-TMS for SCOs has several other very important features. It is where the SCO enters IMS information and creates Invitational Travel Orders (ITO) for the students. The SCO is also able to look up schoolhouse and IMSO point of contact (POC) information. The SCO can also maintain SCO POC information within the SC-TMS so that it is available to the training community. SC-TMS is required to be used for submission of student nomination packages for the Combating Terrorism Fellowship Program (CTFP). The SC-TMS is also used by the SCO to submit the Combined Education and Training Program Plan (CETPP) to the CCMD for approval.

International Affairs Certification Program on the SAN

The SAN currently hosts and provides access to the DOD International Affairs Certification Program (IACP) database. The IACP database is used by program participants to track and to provide a record of certification status.

The IACP was initially instituted by the Defense Security Cooperation Agency in the form of a policy memo in December 2001. This began the long-term process for members of the security cooperation workforce to attain appropriate levels of training, education, and experience to accomplish current-day requirements and better anticipate and prepare for the requirements of the future workforce. In May 2008, the guidance was more formally instituted within DSCA Directive 5012, "Department of Defense International Affairs Certification Program Guidelines."

The current IACP is a voluntary program available to all DOD civilian and military personnel (contractor personnel are not eligible). Personnel who desire to achieve and maintain certification within one of the three tiers of certification are required to complete specific training, education, and experience thresholds and meet basic core competencies associated with the particular tier. Those who attain Tier III certification must continue to earn Continuous Learning Points (CLPs) in order to maintain their Tier III certification.

International-Security Assistance Network and Partner SC-TMS

The International–Security Assistance Network (I–SAN) is a separate portal that is used by the international partner to access the Partner Security Cooperation-Training Management System (PSC-TMS). Using PSC-TMS, the international partner has access to much of the same U.S. international military training data that the SCO sees when they use SC-TMS. Thus, international partner users can view T-MASL data to identify desired courses of instruction and view course descriptions. The international partner has visibility of U.S. international military training that has been requested for their country and the status of that training by viewing the STL. PSC-TMS has the ability for the international partner to enter a limited amount of student biographical information that is electronically passed to SC-TMS for acceptance by the SCO. International customers who would like access to the I–SAN and PSC-TMS should contact their SCO in country. The SCO can then initiate a request for I–SAN and PSC-TMS access for the international partner user via the "Request New I-SAN User" function in the SAN. In addition, International Military Students (IMS) taking the DSCU course, "Security Cooperation Management International Purchaser Financial and Training Management Course" (SCM-IFT), will automatically be given their own I-SAN account with access to PSC-TMS if they do not already have an account. In this course, the student will learn how to operate the I-SAN and PSC-TMS. The I–SAN can be accessed at https://elnath.idss.ida.org/SANweb/.

Financial and Logistics Databases

Financial and logistics databases are maintained by the DFAS, Army, Navy, and Air Force security cooperation agencies. Access to these databases is read-only, unless special permissions are granted. Although it is recognized that SC personnel need access to the data, only those personnel responsible for actions have "write or change" capability. Also, 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 Security Cooperation Accounting (DFAS SCA) in Indianapolis, Indiana, and supported by Enterprise Application Development and Support Division (EADSD) in Mechanicsburg, Pennsylvania. DIFS is the integrated DOD financial system for Security Cooperation cases. DIFS is also the interfacing accounting system that links implementing Agency (IA) financial and logistic records with the FMS Billing Statement (DD 645) and supporting financial documents (e.g., FMS Delivery Listing, etc.) issued to purchasing countries and organizations for the articles and/or services that the country has purchased through the security cooperation case processes.

Functionality

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: https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2875.pdf.

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 the following address and numbers:

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 U.S. Navy's logistics and financial tracking system for security cooperation.

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.

Registration

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

NAVSUP WSS-N5231
ATTN: NAVSUP.MISIL.ADMIN@NAVY.MIL
Philadelphia PA 19111 Fax: (215) 697-0333
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 cooperation programs. CISIL is the central repository for all Army security cooperation 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

CISIL 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. 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 a signed CISIL IT Users Agreement and forward them to the following:

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

Security Assistance Management Information System

System Description

The Air Force Security Assistance and Cooperation Directorate (AFSAC) is responsible for administration of the security cooperation programs within the Air Force Materiel Command (AFMC). Security cooperation 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 cooperation.

Functionality

The SAMIS maintains and reports comprehensive data on AFMC-managed security cooperation programs. This information comes from many different sources; however, most data originates from various Air Force data systems. The SAMIS serves as a repository for FMS case information, requisitions, supply status, shipments, and billing information required by AFSAC to effectively manage security cooperation programs. The SAMIS provides the security cooperation community with accurate and timely information. To accomplish this, the SAMIS provides online, 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 U.S. Government (USG) (including SCOs) and international customers. Access to the SAMIS can be requested via the AFSAC Online website at https://afsac.wpafb.af.mil/register.jsp. Access to the 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 different application formats based upon the category of the user:

- USG—Civilian/Military/Contractor
  - ◊ AFSAC Users—This category includes all personnel directly assigned to AFSAC.
  - ◊ External Users—This category includes ALC employees, AF and DOD supply source employees, USG employees, and contractors, which includes Security Cooperation Officer (SCOs) and employees working in overseas locations such as the Logistics Support Group (LSG).
- Foreign National—Representative/Military/Contractor. This category includes foreign nationals, foreign representatives, and contractors employed directly by the country (i.e., freight forwarder employees, Foreign Liaison Office/Officer [FLO] employees, embassy personnel, and any U.S. citizen employed by a foreign country). Personnel located outside of the U.S. must forward their request for access through their embassy in Washington, DC, unless AFSAC FLO has a delegation letter.

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 cooperation systems. Incorporating an extensive analysis of the security cooperation 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 cooperation 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 a web-based Citrix application only. A SAAR for DSAMS and Citrix access should be completed by the applicant, verified by the applicant's supervisor and security manger, and submitted by the appropriate MILDEP DSAMS point of contact to the DSAMS help desk. The email address is dsca.dsadc.servicedesk@mail.mil and the fax is DSN 430-9082.

Any additional questions should be directed to the following:

DSAMS Help Desk
dsca.dsadc.servicedesk@mail.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 (SCIP)

The Security Cooperation Information Portal (SCIP) is a secure, controlled, unclassified DOD web-based computer information system that provides authorized users with access to Foreign Military Sales (FMS) and Building Partner Capacity (BPC) programs' case-related data and reports to support management responsibilities for those cases. All USG personnel (including Locally Employed Staff (LES) and support contractors) and foreign purchasers (including their authorized freight forwarders) who have job responsibilities requiring access (i.e., need to know) to the SCIP system information are eligible to obtain SCIP accounts. The Defense Security Cooperation Agency (DSCA) encourages USG SC personnel to become familiar with SCIP's capabilities.

SCIP became operational in 2003 and has been significantly expanded and improved over time. SCIP system access (https://www.scportal.us/home/) is available worldwide from any computer (i.e., does not have to be from a USG or DOD domain) as long as there is adequate internet access and an active, authorized SCIP user account.

The SCIP data extracts are obtained (automatically for most of the data) from multiple authoritative DOD and U.S. military department (MILDEP) financial and logistics systems as illustrated in Figure A-1. The majority of data is updated daily via a batch process at 0700 U.S. Eastern Standard Time. Refresh status indicators and information are provided to users in the "Case Information Community" to document the date/time of the last data refresh from those systems.

Prior to the development of SCIP, information relating to the DOD's execution of security cooperation programs was individually available from each of the respective U.S. implementing agencies. The execution information had to be combined by the user to provide a comprehensive tri-service (Army, Navy, and Air Force) view or an entire overview of a country program. In addition, customers did not have access to the tri-service case development system known as the Defense Security Assistance Management System (DSAMS). With SCIP, customers can view DSAMS information relating to their FMS cases. This access allows customers to view DSAMS case status information from the day the case is first initiated in the system for case development work. Perhaps most importantly, SCIP information can be accessed by users worldwide with access to a web browser and the appropriate SCIP account permissions.

Figure A-1
SCIP Authoritative Data Sources

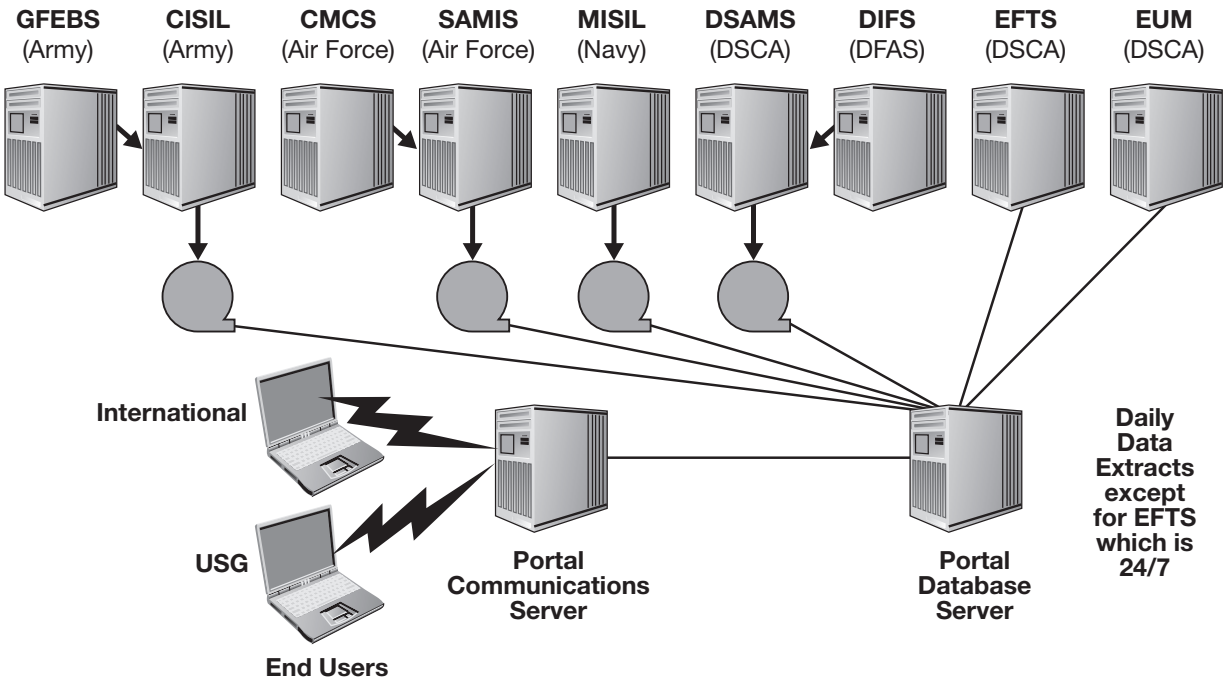
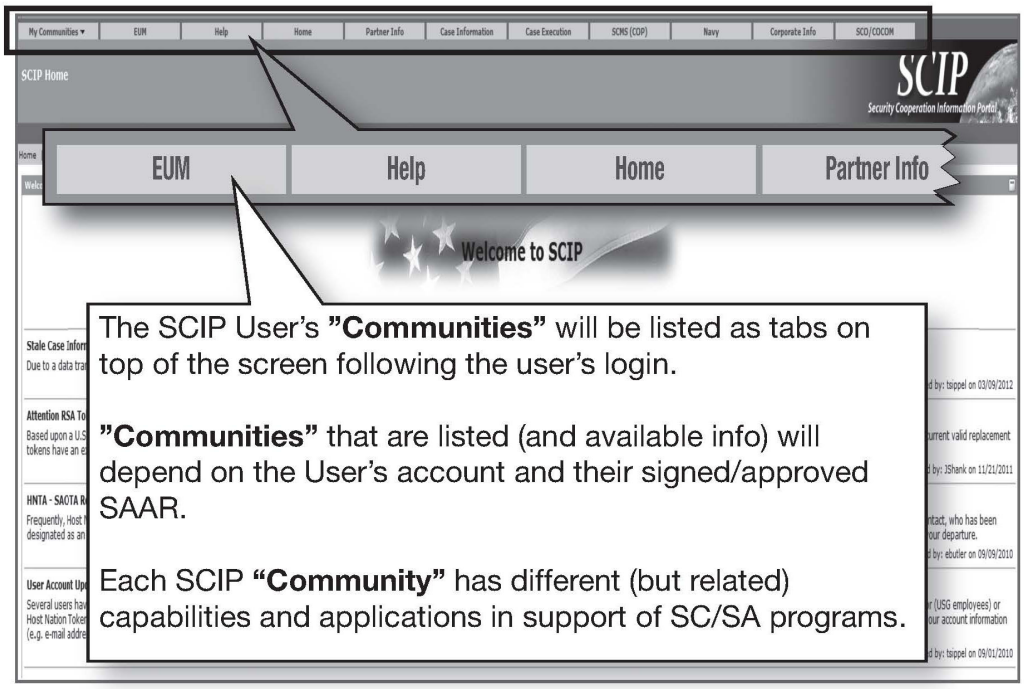


Figure A-2
SCIP Community Menu Bar



Functionality

SCIP enables international customers, customer agents (e.g. freight forwarders, etc.), and USG personnel, with appropriate permissions, to access a variety of features, which are gathered into "Communities" (see Figure A-2). A brief description of the SCIP "Communities" currently available or under development for near term implementation are at https://www.scportal.us/home/docs/SCIP_Background.pdf.

Obtaining a SCIP Account

The online SCIP registration form for both U.S. and international users can be found by accessing the SCIP website (https://www.scportal.us/home/) and clicking the "Registration Info" link on that page. All USG Security Cooperation Office and Geographic Combatant Command students that attend the Defense Security Cooperation University (DSCU) "Security Cooperation Management-Overseas" (SCM-O) course are registered for their individual SCIP accounts while in class per the DSCA Policy Memo 11-58 (Policy Update Regarding Security Cooperation Information Portal [SCIP] Account Access for Security Cooperation Officers [SCOs]).

International (i.e., non-USG) SCIP applicants must be issued a secure SCIP token by their country's Host Nation Token Administrator (HNTA) prior to completing the registration form. DSCA Policy Memoranda 03-11 (Enrollment Process for the SCIP), 05-17 (SCIP Electronic Token Issuance and Replacement Processes), and 14-11 (SCIP Electronic Token Distribution and Replacement Policy) are the policy references for details regarding issuance and management of SCIP tokens. The SCIP International Customer Token Access Guide (https://www.scportal.us/home/docs/SCIP_IntlCust_Access_Guide.pdf) provides further details on SCIP token operations and processes.

All other SCIP account applicants should follow the instructions in the SCIP "Registration Info" introduction to submit the registration for processing by the SCIP Program Office. For additional SCIP assistance, users and prospective users can contact the SCIP Help Desk at dsca.sciphelp@mail.mil.

Accessing SCIP Website

To access the SCIP system once a user has obtained a SCIP account, type https://www.scportal.us/home/docs/SCIP_Background.pdf in the internet browser address line. Various browsers can be used to access SCIP. This system is supported by Microsoft Edge, Google Chrome, and Mozilla Firefox. The browser advanced security settings and DOD root certificates need to be correct to gain access. Also, ensure pop-ups are allowed. Contact the SCIP Help Desk regarding SCIP login issues.

If logging into SCIP with a USG Common Access Card (CAC) certificate, which is the usual means for USG DOD users to login to SCIP if the account has been CAC-enabled, select the non-email certificate. Logging into the SCIP system with a token will be via the subsequent SCIP login screens requiring entry of the SCIP user ID and passcode.

To keep the SCIP account active, users need to periodically logon. The current policy is to suspend user accounts for non-use at 30 days, requiring you to contact the SCIP Help Desk at dsca.sciphelp@mail.mil for account reactivation. At 180 days of non-use, your account will be terminated, requiring you to complete and submit a new registration form to obtain a new SCIP account.

SCIP Training

SCIP user guides and other training resources are available in the SCIP "Help and Training" community.

DSCU provides SCIP training in the majority of its courses. The DSCU classroom SCIP training maximizes the online demonstration of SCIP capabilities by the instructors. Students, then, go online to complete various practical exercises contained within the DSCU SCIP practical exercise handbook. A basic understanding of the SC process, logistics, and finance subjects is needed to understand and interpret the materials and complete the SCIP practical exercises. The SCIP practical exercise can be completed without a SCIP account by using the case examples in the handbook. The SCIP practical exercise handbook is available at http://www.dscu.dsca.mil/documents/publications/scip_practical_exercises_and_handbook.pdf.

Two online SCIP learning guides are available from the DSCU website. The two learning guides are the "Security Cooperation Information Portal (SCIP)" guide and the "SCIP Case Status Demo."

Systems Description

"Socium" (non-acronymous) is an activity lifecycle management system that plans, executes, monitors, and evaluates security cooperation activities. This system is owned and maintained by the Defense Security Cooperation Agency (DSCA) and is to be used by SCOs, GCCs, MILDEPS, IAs, Regional Centers, and other entity that looks to track the lives of security cooperation activities.

It's original premise was to replace the Global Theater Security Management Information System (G-TSCMIS), however Socium's scope is substantially broader than the legacy system. It expands upon G-TSCMIS' event record management by 1) building and streamlining the approval process for Significant Security Cooperation Initiatives (SSCIs) or strategic alignment, (2) version control, collaboration, and development of the Training and Equipment Lists (TELs), (3) converting prose into structured data to enable business analytics, (4) archiving, uploading, and searching community documentation to aid knowledge transfer and records management, (5) centralizing an assessment, monitor, and evaluation (AM&E) framework to house pertinent data points to improve execution, and (6) interfacing with other Authoritative Data Sources to increase knowledge and reduce data-entry.

Functionality

Socium's functionality is determined by the user's role within the application. Users can either view the data or edit the data. "Activity Planners" are tasked with creating and monitoring activities along with "Contributors" they choose to assist them along the way. "Reviewers" are charged with vetting activity data and determining its adequacy for progress along its life cycle. Additionally, there are additional user roles that simply allow users to view all the data that is there. This falls in line with the notion that all users within Socium can view all of its data.

Registration

To obtain access to Socium, prospective users must first submit a completed System Authorization Access Request (SAAR) form. An "Organization Information Owner" (OIO) signature is needed before the request can be sent to the help desk for account creation. There are OIOs embedded into each organization with data within the application. If there is not, that organization must submit a request to the Socium Program Team for authority to designate a member the appropriate permissions to become an OIO.

SUMMARY

Security cooperation personnel have access to numerous automated systems. 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. SC users in the far-flung corners of the 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.

References

DSCA Manual 5105.38-M. *Security Assistance Management Manual* (SAMM). Chapter 13. http://www.samm.dsca.mil/.

DSCA Policy 03-11. *Enrollment for the Security Cooperation Information Portal*. June 25, 2003. https://www.samm.dsca.mil/policy-memoranda/dsca-03-11.

DSCA Policy 5-17. *Security Cooperation Information Portal (SCIP) Electronic Token Issuance and Replacement Processes*. June 24, 2005. https://samm.dsca.mil/policy-memoranda/dsca-05-17.

DSCA Policy 11-08. *Security Cooperation Information Portal (SCIP) Background Document*. February 10, 2011. https://www.samm.dsca.mil/policy-memoranda/dsca-11-08.

DSCA Policy 11-58. *Policy Update Regarding Security Cooperation Information Portal (SCIP) Account Access for Security Cooperation Officers (SCOs)*. November 15, 2011. https://www.samm.dsca.mil/policy-memoranda/dsca-11-58.

DSCA Policy 14-11. *Security Cooperation Information Portal (SCIP) Electronic Token Distribution and Replacement Policy*. October 9, 2014. https://www.samm.dsca.mil/policy-memoranda/dsca-14-11.

SCIP International Customer Token Access Guide. June 2017. https://www.scportal.us/home/docs/SCIP_IntlCust_Access_Guide.pdf.