



DEFENSE SECURITY COOPERATION AGENCY

2800 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2800

15 NOV 2011

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF THE AIR FORCE
FOR INTERNATIONAL AFFAIRS
DEPUTY ASSISTANT SECRETARY OF THE ARMY
FOR DEFENSE EXPORTS AND COOPERATION
DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR
INTERNATIONAL PROGRAMS
CHIEF INFORMATION OFFICER, DEFENSE SECURITY
COOPERATION AGENCY
COMMANDANT, DEFENSE INSTITUTE FOR SECURITY
ASSISTANCE MANAGEMENT

SUBJECT: Policy Update Regarding Security Cooperation Information Portal (SCIP) Account
Access for Security Cooperation Officers (SCOs), DSCA Policy 11-58

Reference: SCIP Account Access for SCOs Background Paper and Action Plan

This memorandum serves as a policy update with regard to the actions and procedures for granting Security Cooperation Information Portal (SCIP) account access to new Security Cooperation Officers (SCOs). These updated procedures will enhance SCO training on SCIP prior to their initial assignments abroad. The primary objective of these changes is to foster greater SCO use of the SCIP system by providing access earlier in the transition process and eliminating paperwork requirements after SCOs arrive at their post. These procedures will become standard practice for the mandatory Security Cooperation Management Overseas (SCMO) training course for all SCOs hosted by the Defense Institute for Security Assistance Management (DISAM).

For any questions concerning this memorandum, please contact Mr. Chris Danielewski, DSCA-STR/POL, at christopher.danielewski@dscamil or (703) 601-4368.

Scott Schless 11/15/2011

Scott R. Schless
Principal Director
For Strategy

Attachment:
As stated

cc:

STATE/PM-RSAT

AFRICOM

CENTCOM

EUCOM

JFCOM

NORTHCOM

PACOM

SOCOM

SOUTHCOM

TRANSCOM

USASAC

SATFA TRADOC

NAVICP

NETSAFA

AFSAC

AFSAT

MDA

Attachment 1

SECURITY COOPERATION INFORMATION PORTAL (SCIP) ACCESS FOR SCOS

PURPOSE: To provide SCIP Access to SCO's at the beginning of course instruction at DISAM to enhance SCO training, functional knowledge, and familiarity with the SCIP system prior to subsequent assignments abroad.

OBJECTIVE: To allow Security Cooperation Officers (SCOs) to have approved access to SCIP and key modules of SCIP during their course of instruction at DISAM, permitting them to then maintain that access as they transition to their new assignments in-country.

ACTIONS PLAN:

1. DSADC will develop and maintain a specialized SCIP Registration form for SCOs. The form will be based on the existing SCIP Registration form pages 1 (Cover page with user name, contact info, etc.) and 2 (Part 1 User Information), and will be capable of being digitally filled in and signed by the SCIP account applicants. DSADC will provide a current copy of that form to DISAM for use by SCM-O students. The form will request SCO access to the communities listed below.
 - i. Case Information
 - ii. Case Execution
 - iii. Partner Information
 - iv. Corporate
 - v. SCO/COCOM
 - vi. SCMS (COP)
 - vii. EUM (Read only)
 - viii. Help
2. DISAM will instruct the SCM-O class on how to apply for individual SCIP accounts at the beginning of that DISAM course. DISAM will also instruct SCM-O students on how to log-in (using their CAC) to their personal SCIP account during the second week of the course in support of their SCM-O SCIP training.
3. DISAM will develop a single MS Excel spreadsheet report, one per SCM-O class, which will provide all information normally found in Part III (Security manager section) of the SCIP Registration form, with a detailed spreadsheet row for each student. DISAM will provide that spreadsheet to (saar@dsadc.dsca.mil), in a single digitally signed and encrypted e-mail, along with all of the individual student registration forms for that class. The spreadsheet providing the security information, and each registration form, will cite the DISAM class number (SCM-O-xx-FY), to allow SCIP access managers to cross-

reference the documents in the future. DSADC will permanently store the electronic forms on protected drives, as it currently stores all SCIP registration artifacts.

4. DSCA/STR will assume sponsorship and responsibility for the Supervisory sections of the SCIP Registration form. This will preclude DSCA/STR from having to subsequently sign individual forms or a cover letter for individual forms. The SCIP PM will develop a document, outlining the proxy signature process, for the SCIP Designated Approving Authority (DAA) signature.
5. DSCA, DSADC, and DISAM Information Technology POCs will identify or develop a computer network based file transfer system that would permit documents (associated with this subject process) to be electronically filed and accessed (with appropriate security protections to ensure that only authorized personnel with a need to know had access) to successfully complete and implement this process in the most efficient means available.

PROCESS PLAN:

The following SCIP account application procedures will be implemented for SCM-O students at DISAM. There are between 45 and 90 students per class (8-9 classes per year). The primary focus of this effort is for students that have been assigned, or are en-route, to SCOs.

DSCA/DISAM/DSADC may, however, also utilize this process for the other remaining DISAM SCM-O class students to maximize the output of this process and increase the USG access to the SCO/COCOM and Corporate Lessons Learned Communities posted on SCIP.

1. On the first day of class, each DISAM SCM-O student will complete the SCIP SCO Registration form with assistance from the DISAM instructor and/or Class Manager as necessary. Students will then digitally sign the completed SCIP SAAR with their CAC and save the completed form to a DISAM designated shared network drive and folder.
2. DISAM will verify each SCM-O student's security clearance and prepare a student listing spreadsheet with a single DISAM signature (from the DISAM Security Manager or Alternate Security Manager) that provides verification (per and IAW Part 3 of the SCO Registration Form) that the listed DISAM SCM-O students (labeled by Class #) are eligible to receive SCIP accounts.
3. DISAM will notify DSCA/STR and DSADC that the signed SCM-O student SCIP Registration form approval (Security Manager and Supervisor) document, and completed/signed SCM-O student SCIP Registration forms, are posted and ready for DSCA/STR and DSADC review and processing. If the shared network system/drive and folder that DISAM, DSCA, and DSADC subject POCs all have access to is unavailable, DISAM will forward those required documents and forms as attachments to the DSADC security manager (saar@dsadc.dsca.mil) via digitally signed and encrypted e-mail(s).
4. DSADC will expedite processing of the account requests.
5. DSADC will initiate student accounts and send individual e-mail notifications to each student who has provided a current USG e-mail address on Page 1 of their SCIP SAAR. DSADC will also provide (via e-mail) the DISAM Registrar with a list of all student

SCIP accounts that have been established. Notifying DISAM will provide complete accountability of the success or failure of the process to the SCM-O Class Managers.

6. The SCO students will utilize their USG CACs to access, with assistance from the DISAM Class Manager and Instructors, their newly established SCIP accounts for both personal training and familiarization, and in support of the DISAM SCM-O SCIP training.
7. Upon arrival in country, each SCO will send a digitally signed email to the SCIP Help Desk at (sciphelp@dsadc.dsca.mil) to update their personal SCIP account information, ensuring that they include their new e-mail address and CAC certificate information changes, if any. Those individuals whose duties require additional functionality or features (e.g. EUM inspection results updating, requisition inputs, etc.) will contact the SCIP Help Desk via email at (sciphelp@dsadc.dsca.mil) to request these capabilities/features.
8. The SCIP Help Desk will coordinate additional capabilities/approvals with the appropriate SCIP Community Information Owners, in accordance with existing procedures.