



DEFENSE SECURITY COOPERATION AGENCY

WASHINGTON, DC 20301-2800

MAR 12 2007

In reply refer to:
I-06/009358-POL

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Information Technology (IT) Governance Board and Change
Review Board (CRB), (DSCA Policy 07-02) [SAMM E-Change 74]

This memorandum updates the Security Assistance Management Manual (SAMM), Chapter 13 to address the establishment of the Information Technology (IT) Governance Board and Change Review Board (CRB). These boards provide a single entry point and review process for all new IT system enhancements and/or system developments for IT systems used by the DoD security cooperation community. The attached change to the SAMM provides guidance on the IT Governance Board and Change Review Board and describes the review process.

This change is effective immediately and will be included in the automated version of the SAMM found on the DSCA Web Page as SAMM E-Change 74. If you have any questions concerning this policy, please contact Ms. Anita Eggleston, DSCA/STR-POL, at 703-601-3843 or e-mail: anita.eggleston@dscamil.

Attachment:
As stated

A handwritten signature in black ink, appearing to read "J.B. Kohler", with a stylized flourish at the end.

JEFFREY B. KOHLER
LIEUTENANT GENERAL, USAF
DIRECTOR

DISTRIBUTION LIST

DEPUTY ASSISTANT SECRETARY OF THE ARMY
DEFENSE EXPORTS AND COOPERATION (DASA-DEC)
DEPARTMENT OF THE ARMY

DEPUTY ASSISTANT SECRETARY OF THE NAVY
INTERNATIONAL PROGRAMS (NAVIPO)
DEPARTMENT OF THE NAVY

DEPUTY UNDER SECRETARY OF THE AIR FORCE
INTERNATIONAL AFFAIRS (SAF/IA)
DEPARTMENT OF THE AIR FORCE

DIRECTOR, DEFENSE LOGISTICS AGENCY

DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

DIRECTOR, DEFENSE REUTILIZATION AND MARKETING SERVICE

DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY

DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

DIRECTOR, DEFENSE LOGISTICS INFORMATION SERVICE

DEPUTY DIRECTOR FOR INFORMATION ASSURANCE,
NATIONAL SECURITY AGENCY

DEPUTY DIRECTOR FOR SECURITY ASSISTANCE,
DEFENSE FINANCE AND ACCOUNTING SERVICE –
DENVER CENTER

Cc: STATE/PM-RSAT
DISAM
USASAC
SATFA TRADOC
NAVICP
NETSAFA
AFSAC
AFSAT

DIILS
EUCOM
SOUTHCOM
PACOM
NORTHCOM
CENTCOM

Security Assistance Management Manual (SAMM), E-Change 74

The SAMM, Chapter 13 is updated as follows:

1. Section C13.1. becomes C13.9. and C13.1 is replaced with the following:

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

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

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

C13.1.2. Information Technology (IT) Governance Board Function. The IT Governance Board meets on a quarterly basis to review and approve all requests for new IT system enhancements and/or system developments or on an ad hoc basis to discuss relevant IT issues. The IT Governance Board ensures all proposed IT system enhancements and/or system developments are necessary and do not exceed current IT budget levels and/or future Program Objective

Memorandum (POM) levels. All new IT system enhancements and/or system developments reviewed and prioritized may not be funded. The IT Governance Board makes the determination of which new IT system enhancements and/or system developments to approve and fund within existing resources allocated to support IT for the security cooperation community. The IT Governance Board only reviews repair/maintenance requests exceeding \$500K.

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

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

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

2. Insert the following new table as C13.T1. and renumber subsequent tables:

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

Step	Action
1 User submits request(s)	Using Figure C13.F1., the user submits all requests to his or her designated IT CRB member, who forwards all requests for new IT system enhancements and/or system developments to the IT CRB for review. All requests for new IT system enhancements and/or system developments that exceed \$500K may require an independent business case analysis as determined by the IT CRB.
2 Review by the IT point of contact or Program Manager	Prior to submission of any IT system enhancement and/or IT system development requests to the IT CRB for review, the IT CRB member must have the appropriate IT point of contact or Program Manager provide a recommendation on the level of effort, technical feasibility, and technical benefit of the proposed IT system enhancement and/or system development. New IT system enhancement and/or system development requests that have not been reviewed by the appropriate IT point of contact or Program Manager will be sent back to the IT CRB member for proper vetting. The applicable IT point of contact or Program Manager maintains and tracks all approved IT enhancements for their IT system and provide updates to the IT CRB.

Step	Action
3 Submissions forwarded to IT CRB chairperson	Upon receipt of the IT point of contact or Program Manager's recommendation, the IT CRB member forwards the request to the IT CRB chairperson for review by the IT CRB.
4 Review by IT CRB members	On a quarterly basis, the IT CRB chairperson consolidates all requests for IT system enhancements and/or system developments and disseminates them to the IT CRB members for review and prioritization. The IT CRB members prioritize each request from a highest to lowest priority using the numbering system (i.e., 1-10) with one being the highest priority. Each request is ranked on its own merit. If an IT CRB member rejects a request this must be indicated as part of the ranking along with the rationale for the rejection. All rejections are discussed by the IT CRB and returned to the submitter along with the rationale for the rejection. If an IT CRB member has questions or concerns regarding a specific request, the IT CRB member notifies the IT CRB chairperson prior to providing the rankings who will determine whether a meeting is required to address the issue. The IT CRB member is responsible for clarifying or adjudicating policy-related questions or requests for policy changes with applicable policy owners. If the requested IT system enhancement and/or system development involves policy changes (e.g., a requested change to or re-interpretation of existing policy), the IT CRB member must return the request to the submitter with a recommendation to contact his or her own policy office for resolution prior to resubmitting the request.
5 Consolidated list forwarded to the IT Governance Board	Upon receipt of the IT CRB members' recommendation of the IT system enhancements and/or system developments, the IT CRB chairperson consolidates the recommendations into a list to be forwarded to the IT Governance Board chairperson (noting all rejections received). For new IT system developments, the IT CRB chairperson notifies the appropriate IT point of contact or Program Manager to prepare a brief for the upcoming IT Governance Board meeting on the proposed IT system development.
6 Review by IT Governance Board	The IT Governance Board meets quarterly to discuss the IT system enhancements and/or system developments on the consolidated list received from the IT CRB or on an ad hoc basis to discuss relevant IT issues. For new IT system developments, the IT point of contact or Program Manager (after Implementing Agency chief information officer review) briefs the IT Governance Board on the proposed IT system's capabilities and overall benefit to the security cooperation community. After review of the consolidated list of IT system enhancements and/or system developments, the IT Governance Board chairperson renders a decision that is recorded and disseminated to the IT CRB chairperson for appropriate action by the applicable IT point of contact or Program Manager. For new IT system developments, the IT point of contact or Program Manager must obtain the IT Governance Board's approval in time for the annual DSCA POM and budget process.

3. Add the following as Figure C13.F1.

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

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

4. Replace sections C13.2.1. in its entirety with the following:

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

5. Replace section C13.2.2. in its entirety with the following:

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

6. Delete section C13.2.3. in its entirety.

7. Replace the following section in Table C13.T1., Security Assistance Network (SAN) Components in its entirety with the following:

SAN Component	Description
International Military Student Office (IMSO) Web and Security Assistance Office (SAO) Web	Tailored to the needs of the IMSO and SAO. Provides access to the same training data used by the Security Assistance Training Community.

8. Replace the following sections in Table C13.T2., Security Assistance Network (SAN) Management Responsibilities in its entirety with the following:

Organization	Responsibility
DSCA (Programs Directorate)	Chair TMS, IMSO Web, and SAO Web Configuration Control Board (CCB).
Defense Institute of Security Assistance Management (DISAM)	Manages and maintains the SAN under the oversight of DSCA (Information Technology Directorate). Manages system administration of the SAN systems and ensures compliance with DoD security and other computer system management requirements. Coordinates appropriate user account administration with the MILDEPs and Combatant Commands. Develops and supports TMS and SAARMS desktop software programs. Publishes and distributes the SAN user's handbooks. Provides initial training to DISAM students and follow-on training. Coordinates the central design and distribution of SAN packages for SAOs. Receives all proposed SAN changes and submits recommended changes through the SAARMS, TMS, or IT CRB as appropriate.

9. Replace sections C13.7.3. and C13.7.4. in its entirety with the following:

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

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

10. Replace section C13.8.1. in its entirety with the following:

C13.8.1. Security Cooperation Information Portal (SCIP) Business Function. The SCIP is managed, administered, and maintained by DSCA (Information Technology Directorate). The SCIP allows security cooperation personnel, including our international partners, to have a tri-Service view of

selected foreign military sales case-related data. The SCIP draws information from the MILDEP Security Assistance legacy systems and is provided to authorized users in a web-based, user-friendly, standardized tool. Users are granted access on a need-to-know basis as determined by their parent organizations (for USG users) or their Government's designated representative (for foreign purchasers). The IT Governance Board via the IT CRB approves all IT system enhancements to SCIP except for repair/maintenance requests under \$500K.

11. Delete sections C13.8.2. and C13.8.3.
12. Renumber current and subsequent sections, tables, and figures in Chapter 13 as required to accommodate above changes.
13. Update the reference list to include the following:
 - (di) Under Secretary of Defense (Acquisition, Technology, and Logistics) memorandum, June 02, 2005, subject: "Investment Review Process Overview and Concept for Operation for Investment Review Boards"
 - (dj) Section 2222 of title 10, United States Code, Defense business systems: architecture, accountability, and modernization