This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

- Purchase this document
- Browse Books & Publications
- Make a charitable contribution

For More Information

- Visit RAND at www.rand.org
- Explore the RAND National Defense Research Institute
- View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.
This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.
A Framework to Assess Programs for Building Partnerships

Jennifer D. P. Moroney, Jefferson P. Marquis, Cathryn Quantic Thurston, Gregory F. Treverton

Prepared for the Office of the Secretary of Defense
Approved for public release; distribution unlimited
The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND’s publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

© Copyright 2009 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND Web site is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (http://www.rand.org/publications/permissions.html).

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN 978-0-8330-4687-1

The research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted in the RAND National Defense Research Institute, a federally funded research and development center sponsored by the OSD, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.
Summary

Security cooperation activities conducted by DoD entities with other nations’ defense organizations range from the very visible—training, equipping, and exercising together—to those that are less obvious, such as holding bilateral talks, workshops, and conferences and providing education. Yet, it is often challenging to determine if these activities have contributed to U.S. objectives—whether at the level of national security, department, COCOM, or service—and if so, by how much or in what ways. Because security cooperation is both dispersed and long-term, it is difficult to measure. At present, program assessments are inconsistent and of varying quality. They may lack objectivity since they are frequently conducted by the organizations that implement the programs. A comprehensive framework for assessing is lacking, although efforts are in place to remedy that deficiency. This project was devoted to that end.

Key Assessment Themes

RAND’s proposed program assessment framework is built around five themes that emerged at a May 2008 assessment workshop that included DoD security cooperation assessment experts, planners, and program managers.

1. **Setting Direction.** An overall goal or set of objectives should be identified for security cooperation activities. The challenge is that most programs support multiple end-states and multiple stakeholders.
2. **Designing Assessments.** Here the issues include assessing both the efficiency of the programs and their ultimate effectiveness as measured against specific security goals.
   - *Building measurable objectives into plans.* Now that the Office of the Secretary of Defense’s (OSD’s) Guidance for Employment of the Force (GEF)\(^1\) calls for program assessment against theater campaign plans, it is essential to design a similar assessment process across COCOMs.
   - *Balancing objective and subjective assessments.* Outcomes-based assessments need to include both types.
   - *Measuring the sustainability of partner capabilities over time.* Too often, assessments stop with immediate outcomes.
   - *Fixing inconsistent language and terminology.* These differences continue to hinder development of standard assessment frameworks across the security cooperation community.

3. **Preparing for Assessment.** The lack of personnel with appropriate assessment backgrounds is a concern, leading to the suggestion of training some experienced assessment professionals who could help programs and COCOMs alike.

4. **Conducting Assessments.** Workshop participants noted the lack of standardized data across COCOMs and programs, the need to reach out for data beyond program managers and U.S. personnel, and the complications of classified information. They suggested establishing either special assessment teams that can be sent into the field or a new, dedicated assessment office.

5. **Explaining Assessments.** This requires both an understanding of how security cooperation programs complement (or impede) other efforts of the military and other government agencies and a better explanation of DoD assessment processes to key audiences and stakeholders.

---

\(^1\) The GEF replaces the OSD Security Cooperation Guidance and was signed by the Secretary of Defense in May 2008.
Key Elements of the Assessment Program Framework

At the highest levels, the National Security Strategy, the National Defense Strategy, the National Military Strategy, the GEF, and the COCOM theater campaign plans form the basis for strategy-driven security cooperation and are key documents in selecting priority partners of interest to the United States. The military departments implement OSD guidance and support the COCOM theater campaign plans by developing their own campaign support plans. In thinking about assessment, stakeholders are critical. For the purposes of this analysis, we defined principal stakeholders as those that are involved with overseeing, planning, or implementing/executing security cooperation programs. In terms of authorities, Title 10 of the U.S. Code serves as the primary authority for many DoD security cooperation programs. Title 22 provides the basic authority for the State Department to oversee and resource security assistance programs, even though they are mostly administered by DoD.

In making assessments, three types of indicators are critical:

- **Inputs** are the resources—both money and manpower—that are required to execute an event.
- **Outputs** are the direct products of an event, activity, or program.
- **Outcomes** are the effect of outputs on the target audience, or changes in program participants’ behavior, knowledge, skills, status and/or level of functioning.

**Metrics** are observable, measurable evidence of outputs and outcomes.

These elements can be combined in a “hierarchy of evaluation” that contains five levels of assessment (see Figure S.1).²

Level 1 is the foundation. Here, evaluation focuses on the problem to be solved or goal to be met, the population to be served, and the kinds of services that might contribute to a solution. Level 2 addresses the design of a policy or program and seeks to confirm that what was planned is adequate to achieve the desired objectives. Level 3 asks

---

whether execution met the design at Level 2. At Level 4, outputs are the products of program activities, and outcomes are the changes that result. This is the first level of assessment at which solutions to the problem that originally motivated the program can be seen. Finally, at Level 5, the assessment looks across programs for cost-effectiveness, or “bang for the buck.”

Assessment Functions
At each level, four functional assessment roles must be performed (although the same organization may perform multiple roles): data collector, assessor, reviewer, and integrator. The data collector is responsible for gathering all relevant information. The assessor sets data collection standards and evaluates the program. The reviewer develops methods and conducts periodic inspections or audits. Finally, the integrator is responsible for organizing and synthesizing programmatic assessments to meet DoD requirements.

Implementing the Assessment Framework
Given multiple stakeholders, these levels of assessment help to determine assessment roles in the same way as stakeholders’ authority influences
their responsibilities, which in turn shape the sets of decisions that fall within their respective purviews. In general, the highest levels of leadership within DoD, typically based on recommendations by OUSD/P, will be responsible for the critical decisions about needs for programs and their design, as well as for assessing cost-effectiveness across programs. The study team recommends that service and COCOM stakeholders should primarily concentrate on matters of process and implementation, as well as on outcomes and impacts.

Many DoD organizations might serve as data collectors, assessors, reviewers, and integrators for OUSD/P-managed security cooperation programs. Table S.1. represents RAND’s notional and proposed organizational assignments as a first step in establishing an integrated structure of assessment roles and responsibilities for DoD. A key goal is to inject a higher level of objectivity into the assessment process and to move away from the current self-assessment approach.

### Table S.1
**Assessment Roles for OUSD/P-Managed Programs**

<table>
<thead>
<tr>
<th>Assessment Decision</th>
<th>Data Collector</th>
<th>Assessor</th>
<th>Reviewer</th>
<th>Integrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Need for program</td>
<td>OUSD/P Partnership Strategy (PS)/ program manager</td>
<td>OUSD/P PS</td>
<td>OSD Program Analysis and Evaluation (PA&amp;E)</td>
<td>OUSD/P PS/DSCA via BPC portfolio manager (BP CPM)</td>
</tr>
<tr>
<td>Level 2: Design/theory</td>
<td>Program manager</td>
<td>Program manager</td>
<td>New OSD SC auditor?</td>
<td>OUSD/P PS/DSCA (via BP CPM)</td>
</tr>
<tr>
<td>Level 3: Process/implementation</td>
<td>Program manager</td>
<td>Program manager</td>
<td>New OSD SC auditor?</td>
<td>OUSD/P PS/DSCA (via BP CPM)</td>
</tr>
<tr>
<td>Level 4: Outputs/outcomes</td>
<td>Program manager</td>
<td>OSD PS</td>
<td>New OSD SC auditor?</td>
<td>OUSD/P PS/DSCA (via BP CPM)</td>
</tr>
<tr>
<td>Level 5: Cost-effectiveness</td>
<td>Program manager</td>
<td>OSD PS</td>
<td>OSD PA&amp;E</td>
<td>OUSD/P PS/DSCA (via BP CPM)</td>
</tr>
</tbody>
</table>

**NOTES:** SC = security cooperation; DSCA = Defense Security Cooperation Agency.
A Proposed OUSD/P Assessment Approach

RAND’s proposed approach seeks to deal with the many obstacles to measuring the effectiveness of BPC and broader security cooperation programs, with the aim of producing assessments that are consistent with the spirit and intent of the GEF. It is meant to provide a useful assessment structure for OUSD/P—specifically for the BPC and other security cooperation programs that are managed directly by OUSD/P. It is also designed to encourage objective analysis.

We propose that OUSD/P consider taking four basic steps:

1. Coordinate with the other major security cooperation players to reach a consensus regarding the definitions of, and linkages among, the key assessment framework elements.
2. Clarify the assessment roles and responsibilities of each program stakeholder by level of assessment.
3. Approve appropriate assessment questions for each level of assessment.
4. Implement a comprehensive security cooperation assessment framework for the programs that OUSD/P directly manages.

Recommendations

To help OUSD/P and DSCA adopt a BPC and, more broadly, a security cooperation assessment framework focused on programs, we lay out the following specific recommendations for implementing the assessment framework in relation to the five themes articulated in this monograph.

Setting Direction

- Work with key DoD stakeholders to clarify program assessment responsibilities in the GEF.
- Build enduring security cooperation goals and measurable program objectives.
- Clarify and standardize assessment terminology.
• Ensure that OUSD/Policy and DSCA are the assessment integrators for programs they manage.

Designing Assessment Processes
• Leverage assessment processes that already exist.
• Within programs, determine stakeholder authorities and roles among the different levels of assessment.
• Consider an assessment function within OUSD/Policy to help implement the assessment framework for OUSD/P-managed programs.

Preparing Stakeholders for Assessment
• OUSD/Policy and OUSD/Personnel and Readiness could work with the Defense Institute for Security Assistance Management and DSCA to develop a professional curriculum for security cooperation assessments.

Conducting Assessments
• Specify stakeholder data collection roles and responsibilities.
• Explore external indicators.
• Standardize assessment questions within and across programs.
• Develop a feedback loop for “setting direction.”
• Consider a pilot program to test the assessment framework.

Explaining Assessment Results
• Develop clearer linkages between assessment and planning.
• Use results to inform decisions about programs.
• Identify examples where multiple, coordinated programs have achieved desired effects.
• Consider using the Global Theater Security Cooperation Management Information System to store program assessments.