

**Global-Theater Security Cooperation
Management Information System
(G-TSCMIS)
Capability Definition Package
25 February 2010**



U. S. Joint Forces Command
Norfolk, VA 23551

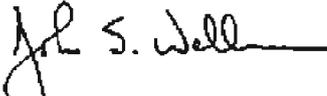
(INTENTIONALLY BLANK)

Global-Theater Security Cooperation
Management Information System (G-TSCMIS)
Capability Definition Package

25 February 2010

Submitted by:

Date: 1 MARCH 2010



JOHN S. WELLMAN

YC-3

Division Chief, Joint Combat Capability Developer (JCCD)

Approved by:

Date:

9 MARCH 2010



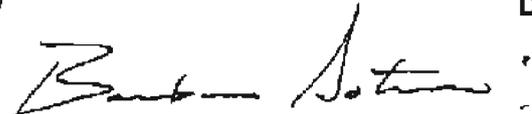
KEVIN J. KENNEDY

Major General, U.S. Air Force

Director, Joint Capability Development

Approved by

Date: 15 March 2010



BARBARA J. SOTIRIN

Deputy Director, Global Security Affairs, J-5, The Joint Staff

Approved by

Date:

20 March 2010



JAMES A. SCHEAR

Deputy Assistant Secretary Of Defense for Partnership Strategy and
Stability Operations

(INTENTIONALLY BLANK)

EXECUTIVE SUMMARY

Per Deputy, Secretary of Defense Memorandum of 10 December 2008, USJFCOM is designated as the functional sponsor for G-TSCMIS and will solicit and rationalize joint G-TSCMIS requirements from Combatant Commands/Services/Agencies (C/S/A) and provide these requirements to the Office of the Secretary of Defense (Policy) and the Joint Staff for approval before formalizing them with the G-TSCMIS acquisition agent.

This Capability Definition Package (CDP)¹ identifies the requirements for G-TSCMIS. It is one of several CDPs that will address the Adaptive Planning and Execution (APEX) capability. This CDP serves to further refine a G-TSCMIS capability with definitions and business process models to ensure development of a capability that meets the C/S/A needs. It also includes a Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF & Policy) "Quicklook" to identify areas that require corrective or supportive actions to ensure the full potential of the materiel solution is realized. This G-TSCMIS capability is intended to provide actionable, decision quality data/information, and operational environment awareness information as a means to support overall Joint C2 and Building Partnerships.

G-TSCMIS will provide a comprehensive picture of whole-of-government Security Cooperation (SC) activities. It will provide decision-makers, SC planners and other users with the ability to view, manage, assess, and report SC activities and events. G-TSCMIS will contribute to planning more effective cooperative security activities to align or meet desired outcomes in support of Security Cooperation (SC) end states. It will support the monitoring, assessment, and allocation of SC funding and assist with identifying redundant SC investments.

– GTSCMIS Vision Statement, Requirements Workshop, 11-13 Aug 2009

As depicted below, SC planning is integral to joint strategic planning. Joint strategic planning provides strategic guidance and direction to the Armed Forces of the United States for SC planning, joint operation planning and force planning.



Figure 1: Joint Strategic Planning Diagram (Joint Pub 5-0).

¹ These capabilities and services are required to support the Key Performance Parameters (KPP); KPP#1 "Shared Situational Awareness" (SSA) and KPP#2 Planning and Execution (found in the Net-Enabled Command Capability (NECC) Capability Development Document (CDD), Increment 1, Change 2, dated 7 June 2007).

(INTENTIONALLY BLANK)

Table of Contents

EXECUTIVE SUMMARY	iii
1. SCOPE	1
2. VISION	2
3. BACKGROUND	2
4. USE NARRATIVE	3
5. REQUIREMENTS	5
6. DOCTRINE, ORGANIZATION, TRAINING, MATERIEL, LEADERSHIP AND EDUCATION, PERSONNEL, FACILITIES, AND POLICY (DOTMLPF AND POLICY) QUICKLOOK	10
6.1 DOTMLPF AND POLICY RECOMMENDATIONS FOR THE G-TSCMIS CDP	11
6.2 TIMING OF SOLUTION DEVELOPMENT.....	13
6.3 RECOMMENDATIONS SUMMARY	13
7. DATA STRATEGY	15
APPENDIX A – SOURCE DOCUMENTS FOR REQUIREMENTS	A-1
APPENDIX B – OPERATIONAL VIEWS/ACTIVITY MODELS	B-1
APPENDIX C – SECURITY COOPERATION AUTHORITATIVE DATA SOURCES (ADS)	C-1
SECURITY COOPERATION ADS ANALYSIS.....	C-1
APPENDIX D – DEFINITIONS AND ACRONYMS	D-1
D.1 DEFINITION LIST	D-1
D.2 ACRONYM LIST.....	D-4
APPENDIX E – REFERENCES	E-1
APPENDIX F - KEY PERFORMANCE PARAMETERS AND KEY SYSTEM ATTRIBUTES	F-1

Figures

Figure 1: Joint Strategic Planning Diagram (Joint Pub 5-0).....	iii
Figure 2: OSD/Joint Staff - Security Cooperation (SC).....	B-1
Figure 3: Assess, Report and Monitor SC	B-2
Figure 4: Develop Concept for SC	B-3
Figure 5: Execute SC Planning.....	B-4
Figure 6: OSD Joint Staff – SC	B-5

Tables

Table 1: G-TSCMIS Requirement Statements.....	5
Table 2: DOTMLPF and Policy Issues	11
Table 3: Additional ADS Owner Initial Requirements.....	16
Table 4: Security Cooperation Information Needs.....	C-1
Table 5: Security Cooperation Data Producers.....	C-3
Table 6: Systems/Tools used by Security Cooperation Data Producers	C-6
Table 7: NECC CDD KPPs.....	F-1
Table 8: NECC CDD KSAs.....	F-3

(INTENTIONALLY BLANK)

1. Scope

The CDP is a tailored product of the Joint Combat Capability Developer (JCCD) that translates warfighter requirements, as written in the Joint Requirements Oversight Council (JROC)-approved Net-Enabled Command Capability (NECC)² Capability Development Document (CDD), into engineering and acquisition useable information which will enable accurate, relevant and timely materiel and non-materiel solution development. G-TSCMIS is an enabler of the APEX process as described in the Adaptive Planning Concept of Operations (CONOPS). This CDP delineates requirements for a G-TSCMIS capability, which will enable DoD organizations (Office of the Secretary of Defense (OSD); Joint Staff (JS); Combatant Commands, Services, and Agencies (C/S/As)) to be able to collect, view, manage and assess Security Cooperation (SC) activities, and be able to share that information within Interagency and multi-national domains, as appropriate. It will provide worldwide visibility of continuously updated SC data, providing open information exchanges and transparency of SC programs (e.g., Foreign Military Sales (FMS), multinational exercises, multinational education) for all SC stakeholders. G-TSCMIS will contribute to the planning of more effective SC activities to align or meet desired outcomes in support of SC end states.

The CDP includes a data strategy section, use narratives and associated architectures which provide operational perspective and context for a G-TSCMIS capability. Additionally, it includes a DOTMLPF and Policy "Quicklook" which identifies key non-materiel issues that, if not resolved, will prevent or degrade the full capability of any materiel solution.

As the functional sponsor for G-TSCMIS, USJFCOM is the focal point for all new and emerging operational command and control (C2) capability needs, including those addressed in the Unified Command Plan (UCP), Joint Planning Guidance (JPG), Guidance for Development of the Force (GDF) and Joint Requirements Oversight Council (JROC) memoranda. USJFCOM defines and articulates detailed requirements from capability needs in order to adopt, adapt or build solutions and integrates and synchronizes DOTMLPF and Policy solutions. USJFCOM established the JCCD to carry out this integration and synchronization function. The JCCD engages and coordinates with warfighters to gather, assess, prioritize, and analyze warfighter C2 requirements. The JCCD articulates current and evolving requirements to capability developers and providers across the DOTMLPF and Policy spectrum to ensure rapid delivery of complete solutions to meet warfighter needs.

² The NECC program has recently been cancelled to be replaced with an approach that sustains and synchronizes the Global Command and Control System (GCCS) Family of Systems (FoS), leverages all applicable NECC products and artifacts, and proposes a programmatic restructuring of a Joint C2 Capability (JC2C).

2. Vision

G-TSCMIS will provide a comprehensive picture of whole-of-government Security Cooperation (SC) activities. It will provide decision-makers, SC planners and other users with the ability to view, manage, assess, and report SC activities and events. G-TSCMIS will contribute to planning more effective cooperative security activities to align or meet desired outcomes in support of SC end states. It will support the monitoring, assessment, and allocation of SC funding and assist with identifying redundant SC investments.

The short term requirement is a global security cooperation management and assessment support tool. In the long term, G-TSCMIS capability will be a fully interoperable component of APEX and the Joint C2 Capability. G-TSCMIS must also be interoperable with other United States Government (USG) foreign assistance and international cooperation information systems. Ideally, it will allow U.S. allies to share information about international security cooperation and capacity building activities. Objectively G-TSCMIS will allow decision makers and analysts to identify redundant investments, plan more effective engagements, and find gaps and opportunities for building more capable partners.

Per the Guidance for the Employment of the Force (GEF), thorough campaign and contingency planning requires that a combatant command's operations and activities align with national security objectives and complement the Department of State's country-specific Mission Strategic Plans (MSP). G-TSCMIS will allow C/S/A and interagency partners to examine U.S. SC engagement and security assistance programs. By having this shared knowledge of C/S/A efforts, DoD leaders can better support the orchestration of whole-of-government efforts and goals.

3. Background

DoD Directive 5132.03 defines security cooperation as "Activities undertaken by the Department of Defense to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DoD interactions with foreign defense and security establishments, including all DoD-administered security assistance programs, that: build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities; develop mission partners' military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations." The GEF and the GDF highlight the strategic importance of improving partners' capacity. This guidance also establishes the requirement for U.S. organizations to build transparent, accountable, and efficient resource management and business processes to track SC data.

The Theater Security Cooperation Management Information System (TSCMIS) is a SIPRNET accessible database that is currently used to record SC activities by all six of the Geographic Combatant Commands (GCC) and two Services (Army and Air Force)³. The USSOUTHCOM model of TSCMIS seamlessly communicates with the USPACOM TSCMIS model, which the other 5 GCCs presently use. DoD requires a Department-wide capability that will enable all components, as well as other Federal Departments, Agencies, and international partners, to see SC data from all sources via a single interface that is tied to each organization's objectives and end states of Country Campaign Plans. This will provide the United States an increased ability to interact with foreign partners to achieve mutual goals of countering terrorism, countering Weapons of Mass Destruction (WMD), promoting stability, and preventing conflict.

On 10 December 2008, the Deputy Secretary of Defense designated the following responsibilities: the Department of the Navy as the acquisition agent, and USJFCOM as the joint functional sponsor. As joint functional sponsor, USJFCOM will provide requirements to OSD (Policy) and the Joint Staff for approval.

4. Use Narrative

The following sample background situation was developed to provide an operational flavor to assist in better understanding the employment of the G-TSCMIS capability:

Use Narrative: A Combatant Commander (CCDR) conducts SC shaping operations within his Area of Responsibility (AOR) in support of a strategic objective to detect and interdict weapons of mass destruction (WMD) that may exist in the possession of specific hostile nations, transnational terrorist organizations, or rogue terrorist actors. This strategic objective is a product of a strategic planning process in which several USG organizations have participated. In addition to DoD, the participants may include Department of State (DoS), Department of Homeland Security (DHS), Department of Justice (DoJ), National Security Council (NSC) and other government agencies as required. Inputs to this strategic planning include the GEF, Joint Strategic Capabilities Plan (JSCP), and the Secretary of State's overall strategic plan for USG foreign policy and developmental assistance. The GEF provides guidance about what the CCDRs should do; the JSCP provides guidance on how they should do it. G-TSCMIS will support strategic planning by providing access to reports of programs, activities, events, funding, assessments, and status of achieving defined end states. Information can be binned by SC programs, budget lines/funding streams, equipment lease, equipment drawdown, etc.

The CCDR directs development of a theater campaign plan to help regional partners build capabilities and capacities to detect and interdict WMD. The campaign plan will identify the ways and means through prioritized SC programs, events, and activities to achieve the CCDR's desired end states. The primary input for the campaign planning process is the assigned mission to help regional partners develop capabilities and capacities to detect and interdict WMD. The CCDR's staff will use the Joint Operation

³ U.S. Navy and U.S. Marine Corps are in the process of acquiring TSCMIS access.

Planning Process (JOPP) and the supporting G-TSCMIS capability, and will involve as additional participants in the planning process its service components, supporting agencies within DoD and mission partners within DoS. Other USG agencies may also participate as required. The campaign plan will produce several operational objectives organized by Lines of Operation (LOO). Each LOO will be populated by programs, activities, and events that are designed to achieve an objective. These will also be further organized into regional and country specific plans. For example, LOO #1 may include developing WMD surveillance capability with foreign militaries, implementing intelligence and information sharing, improving operational access and freedom of action to conduct interdiction, and developing cooperative relationships to create influence contributing to longer-term deterrence and dissuasion. Planners will use G-TSCMIS as a planning support system from which they can draw or propose potential programs, activities, and events that build partners' ability to detect and interdict WMD to inform potential Courses of Action from which a concept of operations is selected. Eventually the LOO within the campaign plan's concept of operations will be populated by these programs, activities, and events, thus providing a demand signal identifying required resources, funding, and authorities for planning and executing SC missions.

Supporting components and agencies will source forces or take other actions to support the specific events and activities that populate the plans to achieve the CCDR's objectives. The various organizations will use the output of the CCDR's campaign plan as the input necessary to conduct their doctrinal planning to support specific events or activities. They will employ their doctrinal planning process to conduct planning, and the output will be the plans for and execution of the programs, force requirements, events, or activities. They will maintain within G-TSCMIS a current SC status that can be reported in numerous ways, to include by type of activity, geographic region or country, U.S. staffing levels, and source or type of funding. Assessment of the execution of plans is conducted by the combatant command staff and component staffs to ascertain the effectiveness of the programs, activities, and events in achieving the objectives of the CCDR's campaign plan. This assessment effort includes the results of each activity or event and the progress in achievement of the strategic end state. The assessment will be linked to the lessons learned system.

G-TSCMIS will support visualization, assessment, reporting, and data management throughout the conduct of SC planning and execution. Reports will be tailored to include programs, events, and activities by category, geographical areas, assessments, U.S. staffing levels, and sources of funding. Users at the tactical level will focus on specific programs, participating forces, events, and activities, while users at the strategic level can access summary reports of geographic regions, resource requirements, or total expenditure of funds by source. G-TSCMIS support to DoD's SC reporting requirements is particularly important. Reporting requirements for many SC programs and activities are mandated by federal law.

5. Requirements

USJFCOM hosted a 3-day G-TSCMIS Requirements Workshop on 11-13 August 2009 in Suffolk, VA. All combatant commands, Services, and applicable defense agencies were invited to participate in the identification of requirements for G-TSCMIS. The following table was developed from C/S/A inputs received at that workshop and from extant documents from the existing TSCMIS and Army Global Outlook System (ARGOS).⁴ Each of the requirement statements has been directly linked to the Net-Enabled Command Capability (NECC) Capability Development Document (CDD).

Table 1: G-TSCMIS Requirement Statements

#	Draft G-TSCMIS Requirement Statements	NECC CDD Linkage
11.1	G-TSCMIS shall comply with DoD Information Assurance directives, policies, and instructions.	9.6
11.2	G-TSCMIS shall protect and defend shared information/resources by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.	9.6
11.3	G-TSCMIS shall provide an access control methodology based on assignment of individual attributes, and/or the aggregation of any number of existing or additional attributes, to resources and identities; enabling tailored access control to information/resources.	9.6
11.4	G-TSCMIS shall provide the capability to track all user actions (e.g., access requests, create, read, update, delete)	9.6
11.5	G-TSCMIS shall provide the capability to prevent unattributed modification of information/resources.	9.6
11.6	G-TSCMIS shall provide attribute-based access control (ABAC) ⁵ to provide user authentication and identify associated permissions for information/resource access.	9.1, 9.4, 9.5, 9.6, 9.7
11.7	G-TSCMIS shall provide the capability for a single sign-on for access to multiple sources of data.	9.1, 9.2, 9.4, 9.5, 9.6, 9.7
11.8	G-TSCMIS shall provide an embedded, 24-hour available, online help capability (e.g., intuitive and contextual-based help menus, self-service knowledge repository, and human-interactive help desks) supporting 24/7 education and training of units and individuals dispersed temporally and geographically.	9.1, 9.3, 9.7
11.9	G-TSCMIS shall provide the capability to develop standardized and easily understood course materials to deliver training to the warfighter on a variety of platforms operating in diverse environments (classroom to work center) with the same look and feel whether conducting classroom, web-based, or computer-based training.	9.3
11.10	G-TSCMIS shall provide the capability to develop standardized and easily understood course materials to deliver training to the warfighter that meets Advanced Distributed Learning Sharable Content Object Reference Model (SCORM) standards.	9.3

⁴ Refer to Appendix A for a listing of supporting documents used to develop/refine requirements for G-TSCMIS.

⁵ Attribute-Based Access Control (ABAC) is an access authorization policy model that allows the system to take all, or any subset of, attributes into consideration when vetting a request for access to the system. The ABAC approach does not require specific role definitions; instead, policies are based on binary conditions associated with the attributes in an individual's profiles, the system resource constraints, and environmental conditions (such as threat levels, network conditions, network security classifications, etc.).

ID	Draft G-TSCMIS Requirement Statements	NECC CDD Linkage
11.11	G-TSCMIS Shareable Content Object Reference Model (SCORM)-conformant products will be registered on the Advanced Distributed Learning Registry (ADL-R) to support rapid search, discovery, retrieval and re-use.	9.3
11.12 ⁶	G-TSCMIS shall provide the capability to manage (Create, Read, Update, Delete) Security Cooperation (SC) event data: Event Title, Identifier Field, Fiscal Years, US Only Event, Event Sub Types, Engagement categories, Points of Contact/Office of Primary Responsibility (OPR), Key Organization Data, Event Status, Event Execution Dates, Classification/Releasability, Remarks, Description, Additional Comments, Military Engagement Themes, Event Series, Locations, Participating Country(ies), Participating US Units, Other Supporting Elements/Offices, Number of Scheduled Military/Civilian Participants, Number of Actual Military/Civilian Participants, Required Resources/Funding Resources, Theater Strategic Objectives/Country Objectives/SC Desired Effects, Event Milestones, Administrative Events, Assessments, Assets.	1.1, 1.3, 4.1, 5.1, 6.2, 9.1, 9.7
11.13	G-TSCMIS shall provide the capability for users to create and manage additional SC event reporting criteria.	9.1
11.14	G-TSCMIS shall provide the capability to enter SC event data via standardized data entry selections (e.g., pull-down menus, lists, tables).	1.1, 1.3, 4.1, 5.1, 6.2, 9.1, 9.5, 9.7
11.15	G-TSCMIS shall provide the capability to perform a validation check on an SC event to ensure that all required fields have been completed.	9.4, 9.7
11.16	G-TSCMIS shall provide the capability to designate certain SC event data fields as "required" data fields (which must be filled in for the event to pass the validation check).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.17	G-TSCMIS shall provide the capability to embed supporting documents to an SC event record.	9.1, 9.7
11.18	G-TSCMIS shall provide the capability to create a symbolic relationship or link (e.g., a Uniform Resource Identifier (URI) or a Uniform Resource Locator (URL)) into an SC event record.	9.1, 9.7
11.19	G-TSCMIS shall provide a capability to record in an SC event record compliance with applicable Laws, Regulations and Policies by the appropriate oversight organization for an SC activity/event.	1.1, 1.3, 9.1, 9.7
11.20	G-TSCMIS shall provide the capability to copy an already developed SC event and use it as a template for another SC event.	1.1, 1.3, 9.1, 9.4, 9.7
11.21	G-TSCMIS shall provide the capability to copy data from an SC event record text field.	1.1, 1.3, 9.1, 9.4, 9.7
11.22	G-TSCMIS shall provide the capability to paste data into an SC event record text field.	1.1, 1.3, 9.1, 9.4, 9.7
11.23	G-TSCMIS shall provide a capability to import data using standard formats (e.g., Comma Separated Values (CSV), Microsoft Excel) for data input.	1.1, 1.3, 9.1, 9.4, 9.7
11.24	G-TSCMIS shall provide the capability to perform a search within G-TSCMIS.	9.1, 9.7
11.25	G-TSCMIS shall provide the capability for a user to perform specific, custom queries using filters and selection criteria.	9.1, 9.7

⁶ The data fields listed in this requirement statement represent current TSCMIS/ARGOS reporting criteria.

#	Draft G-TSCMIS Requirement Statements	NECC CDD Linkage
11.26	G-TSCMIS shall provide the capability for a user to sort by any data field (e.g., by OPR or executing component).	9.1, 9.7
11.27	G-TSCMIS shall provide a capability for a single point of data entry capability (to preclude the necessity for agencies/Services to establish separate accounts with each Geographic Combatant Command (GCC)).	1.1, 1.3, 4.1, 5.1, 6.2, 9.1, 9.7
11.28	G-TSCMIS shall provide a capability for an SC event manager to grant permission to allow multiple commands/organizations to enter their SC data against a single SC event.	1.1, 1.3, 4.1, 5.1, 6.2, 9.1, 9.7
11.29	G-TSCMIS shall provide the capability to access data from Authoritative Data Sources (ADS) (e.g., Defense Security Assistance Management System [DSAMS], Security Assistance Network [SAN], Joint Training Information Management System [JTIMS], Training Management System [TMS], Joint Capability Requirements Manager [JCRM], Global Force Management tool), including authoritative SC references.	1.1, 1.3, 2.1, 3.1, 4.1, 9.1, 9.2, 9.6, 9.7
11.30	G-TSCMIS shall provide interoperability with existing fielded SC systems and planning systems.	1.1, 1.3, 2.1, 4.1, 9.1, 9.2, 9.6, 9.7
11.31	G-TSCMIS shall provide the capability to expose SC data, in accordance with CJCSI 6212.01E ⁷ .	1.1, 1.3, 2.1, 4.1, 9.1, 9.2, 9.6, 9.7
11.32	G-TSCMIS shall provide a capability to operate in an unclassified environment.	1.1, 1.3, 2.1, 4.1, 9.1, 9.2, 9.6, 9.7
11.33	G-TSCMIS shall provide a capability to operate in a classified environment.	1.1, 1.3, 2.1, 4.1, 9.1, 9.2, 9.6, 9.7
11.34	G-TSCMIS shall provide the capability to access and transfer SC data (within security classification guidelines) across multiple security levels/domains.	1.1, 1.3, 2.1, 4.1, 9.1, 9.2, 9.6, 9.7
11.35	G-TSCMIS shall provide the capability to display linkages between: SC activities, SC objectives, intermediate military objectives, theater strategic objectives, Guidance for Employment of the Forces (GEF) strategic end states, Theater Campaign Plan objectives, Mission Strategic Plan (MSP) by country, resources, non-DoD participants, etc.	1.1, 1.3, 4.1, 5.1, 6.2, 9.1, 9.7
11.36	G-TSCMIS shall provide a capability for schedule management and resource allocation (e.g., Microsoft Project).	1.1, 1.3, 2.1, 9.1, 9.4, 9.7
11.37	G-TSCMIS shall provide a capability for planning SC activities/events.	1.1, 1.3, 9.1, 9.4, 9.7
11.38	G-TSCMIS shall provide a capability to enable supporting commands/Services/agencies to build projections for future SC resource requirements (e.g., participating forces, funding).	1.1, 1.3, 2.1, 9.1, 9.4, 9.7
11.39	G-TSCMIS shall provide a future capability to conduct analysis of opportunities for engagement and linked to Guidance for Employment of the Force (GEF) and/or CCDR goal/objectives.	9.9

⁷ Link to CJCSI 6212.01E: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf

#	Draft G-TSCMIS Requirement Statements	NECC CDD Linkage
11.40	G-TSCMIS shall provide the capability to notify Joint Force providers and Service resource providers of potential Requests for Forces (RFF) as SC events are planned.	1.1, 1.3, 2.1, 9.1, 9.4, 9.5, 9.7
11.41	G-TSCMIS shall provide an automatic notification to appropriate individuals/organizations of required SC tasks and assignments.	1.1, 9.1, 9.5, 9.7
11.42	G-TSCMIS shall provide users the capability to subscribe to electronic alerts when additions or changes are made in selected categories.	1.1, 9.1, 9.5, 9.7
11.43	G-TSCMIS shall provide a capability to guide an action officer through required steps of SC activity planning and reporting.	1.1, 9.1, 9.3, 9.4, 9.7
11.44	G-TSCMIS shall provide a capability for operators to utilize synchronous and asynchronous collaboration tools (e.g., Social Networking Services (SNS), Smartboards, wikis, chat, e-mail).	9.1, 9.2, 9.5, 9.7
11.45	G-TSCMIS shall provide the capability to export SC data into standard word documents.	9.4, 9.7
11.46	G-TSCMIS shall provide the capability to export SC data into spreadsheets.	9.4, 9.7
11.47	G-TSCMIS shall provide a capability to build and export calendar views.	9.4, 9.7
11.48	G-TSCMIS shall provide a message board/posting capability for users to make posts and discuss events to capture qualitative data that would not otherwise be apparent in the data collection and recording process.	9.4, 9.7
11.49	G-TSCMIS shall provide the capability to export SC data into standard visual presentation documents (e.g., Power Point).	9.4, 9.7
11.50	G-TSCMIS shall provide the capability to export SC data into a visualization tool.	4.1, 9.4, 9.7
11.51	G-TSCMIS shall provide a capability to display historical, current and future planned SC events (with amplifying data) on an interactive mapping tool (such as Google Earth) via user-defined criteria such as timeframe, objective, country, agency.	1.1, 1.3, 4.1, 9.4, 9.7
11.52	G-TSCMIS shall provide a capability to synchronize and display SC information from multiple Combatant Commands/Services/agencies.	1.1, 1.3, 4.1, 9.2, 9.4, 9.7
11.53	G-TSCMIS shall provide a capability to display all the SC activities of an individual agency or command or Service within a particular country or user-defined region.	1.1, 1.3, 4.1, 9.2, 9.4, 9.7
11.54	G-TSCMIS shall provide a capability to customize a display to assist with planning and tracking activities/events (e.g., roll up/dashboard view).	1.1, 1.3, 4.1, 9.2, 9.4, 9.7
11.55	G-TSCMIS shall provide a capability to display resources that have been allocated to specific SC activities/events.	1.3, 2.1, 4.1, 9.1, 9.2, 9.7
11.56	G-TSCMIS shall provide a capability to track and display expenditure of funds by sources (e.g., Title 10, Title 22, Section 1206) and activities.	9.1, 9.7
11.57	G-TSCMIS shall provide a capability to display allocation of resources (funding, forces, equipment) for an SC program/event/activity in terms of goals/objectives/end states.	1.3, 2.1, 4.1, 9.1, 9.2, 9.7
11.58	G-TSCMIS shall provide a capability to display linkages between the resource allocation of multiple programs and a single theater strategic objective/strategic effect.	1.3, 2.1, 4.1, 9.1, 9.2, 9.7

#	Draft G-TSCMIS Requirement Statements	NECC CDD Linkage
11.59	G-TSCMIS shall provide a capability to display expenditure of resources for an SC program/event/activity in terms of goals/objectives/end states.	1.3, 2.1, 4.1, 9.1, 9.2, 9.7
11.60	G-TSCMIS shall provide a capability to display linkages between resources and Guidance for the Employment of Forces (GEF) priorities.	1.3, 2.1, 4.1, 9.1, 9.2, 9.7
11.61	G-TSCMIS shall provide the capability to process security cooperation event data and report summaries of funding and/or manpower required by funding category, by country, by region, by objective, etc.	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.62	G-TSCMIS shall provide the capability to create charts and graphs of SC data (e.g., Gantt charts, pie charts, bar graphs).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.63	G-TSCMIS shall provide the capability to access standardized reports for SC events.	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.64	G-TSCMIS shall provide the capability to generate an Events Summary report (e.g., by SC category, by country).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.65	G-TSCMIS shall provide the capability to generate Quality Assurance (QA) reports (e.g., Agency, Country, Points of Contact) for SC activities, in order to identify and correct missing/incorrect information for the user.	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.66	G-TSCMIS shall provide interactive Quality Assurance (QA) reports that allow the user to directly navigate to an SC event record which has been identified (flagged) for QA non-compliance.	9.1, 9.4, 9.7
11.67	G-TSCMIS shall provide a capability to notify a user that an SC event record has an incorrect status (i.e., an event start and/or end date has passed and the event status has not been updated).	9.1, 9.5, 9.7
11.68	G-TSCMIS shall provide the capability to generate Analytical reports (e.g., Agency to Engagement Category, Agency to Event Status, Events to Country Objectives/Sub Objectives, Country to Engagement Category, and Country Sub Objectives to SC Events).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.69	G-TSCMIS shall provide the capability to generate Monthly reports (e.g., by country or agency).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.70	G-TSCMIS shall provide the capability to generate Executive Overviews (e.g., agency overview, agency to country overview, country overview, country group overview).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.71	G-TSCMIS shall provide a capability to automatically produce a fact sheet that provides summary information (who, what, when, where, why, how, historic examples, lessons learned, and event prerequisites) about a particular SC activity/event.	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.72	G-TSCMIS shall provide a capability to automatically produce a report in various required formats (e.g., the National Security Council's Significant Military Exercise Briefing (SMEB) format).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.73	G-TSCMIS system shall collate and categorize completed event assessments for use by planners, managers, analysts and decision makers.	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.74	G-TSCMIS shall provide the capability for SC participants to generate Event Assessment reports.	1.1, 1.3, 4.1, 9.1, 9.4, 9.7
11.75	G-TSCMIS shall provide a capability to produce, by Guidance for the Employment of the Force (GEF) categories, an assessment of how SC activities achieved themes and objectives identified in the GEF (based on a user-defined timeframe).	1.1, 1.3, 4.1, 9.1, 9.4, 9.7

#	Draft G-TSCMIS Requirement Statements	NECC CDD Linkage
11.76	G-TSCMIS shall provide a capability to perform an Event Assessment upon completion of an SC event to include: ratings for event execution, assessment for event success in support of engagement objectives, and an opinion on event scope/frequency (i.e., increase, decrease or maintain current level).	9.1, 9.4, 9.7, 9.10
11.77	G-TSCMIS shall provide a capability that displays how SC activities are progressing towards achievement of goals/themes/objectives/end states.	1.1, 4.1, 9.1, 9.2, 9.7, 9.10
11.78	G-TSCMIS shall provide a capability to compare/deconflict DoD SC activities with non-DoD activities to identify duplicative efforts and to assist with allocating future resources towards achieving desired objectives/end states.	9.1, 9.2, 9.7, 9.10
11.79	G-TSCMIS shall provide modeling tools which predict effects of applying future resources towards meeting SC objectives (i.e., predict return on investment).	4.1, 9.10
11.80	G-TSCMIS shall provide a capability to identify and request future funding requirements based on various budgeting cycles (e.g., Program Objective Memorandum (POM), Foreign Military Financing (FMF), Mission Strategic Plan (MSP), International Military Education and Training (IMET)).	9.1, 9.7
11.81	G-TSCMIS shall provide a capability to prioritize SC events.	9.1, 9.7, 9.10
11.82	G-TSCMIS shall provide a capability to visualize priorities of SC events against resources.	9.1, 9.7, 9.10
11.83	G-TSCMIS shall provide the capability to operate in a Disconnected, Intermittent, or Limited bandwidth (DIL) environment.	9.7
11.84	G-TSCMIS shall provide the capability to electronically approve SC events.	1.3, 9.1, 9.7

6. Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF and Policy) Quicklook

The DOTMLPF and Policy quick-look section of this CDP identifies issues articulated from the start of research through the writing and staffing of this document. This includes all DOTMLPF and Policy issues identified during research, meetings with warfighter subject matter experts (SMEs) and CDP staffing at the JCCD level. Most of the issues were identified by warfighters – current TSCMIS and ARGOS⁸ users at the combatant commands and Services. The primary basis for selection and emphasis was whether solving the issue would enhance the use of G-TSCMIS materiel capabilities. Another basis was whether the adoption of a non-materiel solution, relative to G-TSCMIS's materiel capabilities, would enhance the SC application for the warfighter. Experience in the fielding of several previous joint systems has demonstrated negative impact when primary emphasis is given to the development and implementation of a materiel solution and insufficient effort is given to the non-materiel solutions such as

⁸ ARGOS is a Service implementation of the USPACOM TSCMIS (P-TSCMIS) model presently used by Army and Air Force.

policy, doctrine, training, etc. The result was that the new system was seriously hampered or not used at all until lessons learned and the passage of time brought about necessary support changes.

This DOTMLPF and Policy Quicklook section of the G-TSCMIS CDP articulates the nature of non-materiel (and some materiel) issues identified in the research and staffing of the CDP. The Quicklook also makes specific recommendations to identified commands or agencies, hereafter referred to as DOTMLPF and Policy developers, to research each issue and recommendation as stated in the CDP and produce solutions in time to meet events in the testing, fielding and warfighter utilization of G-TSCMIS.

6.1 DOTMLPF and Policy Recommendations for the G-TSCMIS CDP

The following table summarizes the subjects of each of the DOTMLPF and Policy area(s), findings, recommendations, and the suggested Offices of Primary Responsibility (OPR)/Offices of Collateral Responsibility (OCR) for carrying out the recommendations.

Table 2: DOTMLPF and Policy issues

DOTMLPF and Policy Issue	Finding	Recommendation	Suggested OPR/OCR
Doctrine Policy	JP 5-0 provides insufficient doctrine on Theater Campaign Plan development and guidance to link SC planning activities and campaign planning.	JS J5 produce a doctrinal publication in the JP-5 (planning) series to address campaign planning. Make appropriate changes to: CJCSM 3122.01A, <i>Joint Operation Planning and Execution System (JOPES), Volume 1, (Planning Policy and Procedures)</i> , 29 Sep 08. CJCSI 3141.01D, <i>Management and Review of Campaign and Contingency Plans</i> , 24 Apr 08.	JS/J5

Doctrine Policy	JP-5 series provides insufficient doctrine on the planning of Theater Security Cooperation.	JS J5 produce an additional doctrinal publication in the JP-5 series to address theater security cooperation planning. Make appropriate changes to: <i>Guidance for Employment of the Force (GEF)</i> , 21 Apr 08; <i>Joint Publication 3-08, Interorganizational Coordination during Joint Operations</i> , 17 Mar 06; <i>Joint Publication 5-0, Joint Operation Planning</i> , 26 Dec 06; <i>Military Contribution to Cooperative Security Joint Operating Concept (CS JOC)</i> , 19 Sep 08; <i>Joint Publication 1-02, DOD Dictionary of Military and Associated Terms</i> (as amended through 19 Aug 09).	JS/J5 JS/J3 OSD
Organization Leadership	OSD and DSCA provide overarching governance of SC policy and planning; however, no coordination and resolution body exists.	JS J5 initiate a Community of Interest or Working Group.	JS/J5
Organization Leadership	No formal program management office exists to address critical issues with current TSCMIS system and management of follow-on G-TSCMIS system.	Formally appoint a program management office for G-TSCMIS.	OSD
Training Organization	Need to establish a single training management authority to coordinate all related training requirements, course curricula, and training providers.	Coordinate with DSCA & DISAM to develop SC planning courses for GCCs/Services. Broaden DISAM's mission to include instruction on SC planning.	OSD DISAM DSCA JS
Training Personnel	Lack of training for personnel assigned SC planning responsibilities.	JS and Services update and enhance Security Cooperation training for personnel assigned to joint commands. Specific common training requirements should be developed. Coordinate/integrate SC planning training requirements with the APEX Human Resource Strategy. Make appropriate changes to <i>CJCSI 1001.01, Joint Manpower and Personnel Program</i> , 17 Mar 08.	JS/J7 Services

Leadership/ Education Policy	Lack of SC exposure and supporting systems to Senior Leaders.	Make curriculum changes at JFSC and senior service schools. Brief the new FO/GOs at Capstone. Make appropriate changes to CJCSI 1800.01D, Officer Professional Military Education (PME) Policy, 15 Jul 09.	JS
Policy	Lack of sufficient policy and guidance to implement/ manage SC planning activities and information exchanges in an unclassified environment.	OSD and the JS develop appropriate guidance.	OSD JS
Policy	Lack of guidance on how DoD systems will interoperate with non-DoD systems.	Update CJCSI 3141.01D, CJCSM 3122.01A and other directive joint policy documents to enforce use of G-TSCMIS capability as required.	OSD JS

6.2 Timing of Solution Development

Most of these DOTMLPF and Policy areas require the review of a broader scope of data. Consequently, delivery of the revised documentation may not coincide with materiel releases. This requires close synchronization between the developer, JCCD, and individual DOTMLPF and Policy developers to ensure delivery of critical DOTMLPF and Policy support precedes the delivery of materiel solutions.

6.3 Recommendations Summary

G-TSCMIS provides a series of improvements over the current capabilities now in use by warfighters. Inevitably this results in changes to lower-level procedures and processes and may result in important changes in upper-level doctrine concerning the planning and conduct of theater security cooperation. Moreover, all other areas of DOTMLPF and Policy will be impacted to some degree.

DOTMLPF and Policy recommendations contained in this document, and as changed or added to by future analysis of testing, represent capability gaps that must be resolved and provided to the joint warfighter on a reasonably concurrent schedule with the delivery of materiel capabilities.

The most significant DOTMLPF and Policy recommendations contained in this document are:

- **Doctrine:** Update joint and Service doctrine at all levels to reflect not only the CCDRs' requirements to conduct and execute SC planning, but also Service and Defense agencies' role in supporting CCDR SC and their requirement to conduct SC activities in the accomplishment of their respective missions. Incorporate and mandate the use of G-TSCMIS in these updates.

Specifically, there is a gap in joint doctrine related to both campaign planning and SC planning. These terms are not synonymous and should be addressed in separate publications within the planning series of joint doctrine. SC planning should include the roles and responsibilities of combatant commands and their service components in the planning, execution, and assessment of SC. It should also include the roles and responsibilities of OSD, the Joint Staff, and the Service headquarters in SC. Finally, the new doctrine must explain the roles and relationships of interagency partners such as Department of State, to include embassies, Department of Justice, and other agencies that provide assets.

SC planning doctrine should explain the relationship between strategic goals, operational planning, and tactical execution of the events and activities that populate country specific or region specific campaign plans. The doctrine must also explain the urgent need to conduct assessment of both specific activities and the overarching campaign plan in achieving the plan objectives that are linked to strategic goals.

- **Organization:** Following the August 2009 G-TSCMIS Requirements Workshop, warfighters have formed an informal Community of Interest (COI) for G-TSCMIS to identify best practices, coordinate user efforts and activities, and develop the required COI products (controlled vocabulary, etc). This initiative could be further enhanced by formally establishing a COI with a charter, channels of communication, etc.

- **Training:** Provide Sharable Content Object Reference Model (SCORM) compliant training, per DoDI 1322.26, at the functional/technical levels and provide/update training at the schoolhouse and combatant command levels. Both need to reflect the requirements and capabilities provided by G-TSCMIS as a system that supports TSC. Also consider establishment of a Training Management Authority (TMA) to consolidate and integrate training packages produced during materiel development and to distribute standardized SC and G-TSCMIS curricula to joint and Service training establishments.

- **Materiel:** Develop the system to conform to Government off-the-Shelf (GOTS) hardware standards such that the system functions across the spectrum of DoD and interagency organizations. Enforce standardized data for the G-TSCMIS. Further, build into the system the ability to interface with other systems, such as Joint Training Information Management System (JTIMS), Joint Capability Requirements Manager (JCRM) and Defense Readiness Reporting System (DRRS), necessary to manage the force to source SC requirements.

- **Leadership:** Update Joint Professional Military Education (JPME) at all levels to reflect the requirements, capabilities and opportunities provided by G-TSCMIS. Further, JPME and Service PME should include the fundamentals of both the process of campaign planning and the principles of SC. As an additional leadership consideration, OSD and the JS need to take action on numerous issues of policy that affect both SC and G-TSCMIS.

- **Personnel:** Update manning document requirements for personnel qualifications at all joint levels to reflect the training and JPME requirements and capabilities provided by G-TSCMIS.

- **Policy:** Several policy issues need resolution to support development and fielding of G-TSCMIS. Foremost among these are the policy requirements for DoD and interagency coordinated action in the conduct of planning and execution of SC. There are conflicting and confusing policies and laws that apply to the many SC activities. An extended requirement is created as G-TSCMIS will allow multi-agency users web-based access. There will also be information assurance issues such as data security and access due to the sensitivity of the contents of the system. This may require SIPRNET vice NIPRNET access similar to the current TSCMIS tool.

7. Data Strategy

G-TSCMIS developers must comply with all federal/state laws, regulations, and DoD policies, including data and service exposure in accordance with Defense Information Enterprise Architecture (DIEA) v1.0 (11 April 2008), Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, and Health Insurance Portability and Accountability Act (HIPAA) for Personally Identifiable Information (PII).

DIEA Data and Services Deployment (DSD) sections describe a net-centric vision that provides a rich information sharing environment in which data and services will be widely available, easily discoverable, usable and trusted across the Global Information Grid (GIG). CJCSI 6212.01E provides further detailed guidance. Enclosure E of CJCSI 6212.01E describes the technical aspect of determining Interoperability and Supportability, including the Net-Ready Key Performance Parameter (NR-KPP) and compliance with DoD IT and National Security Systems (NSS) specific policies. CJCSI 6212.01E incorporated compliance with Net-Centric Data and Services Strategy, including Data and Service Exposure Verification, as one of the five elements of the NR-KPP. Inclusion of the NR-KPP is mandatory for all acquisition and post acquisition IT and NSS programs for systems used to enter, process, store, display, or transmit DoD information, regardless of classification or sensitivity, except those that do not communicate with external systems. See CJCSI 6212.01E for further NR-KPP guidance.

In addition to the requirements in DIEA and CJCSI 6212.01E, the C2 CPM has identified additional ADS owner initial requirements, as directed by JROCM 158-09 (Table 3) to ensure that the data provided by ADS owners meet warfighter requirements. These requirements include: 1) Document the data services provided and conditions of those services; including availability, data freshness and query performance; 2) Maintain physical & system security/safeguards appropriate to classification of the data in the ADS; 3) Ensure that data quality standards are developed and implemented; and 4) Maintain Disaster Recovery plans and facilities adequate to maintain or restart operations in the event systems or facilities are impaired, inaccessible, or destroyed.

Table 3: Additional ADS Owner Initial Requirements

Services Provided and Conditions of Service
<ul style="list-style-type: none">▪ An Availability Service Level Agreement defines the operating hours during which the ADS is "open for business" on a regular basis.
<ul style="list-style-type: none">▪ A Data Freshness Service Level Agreement defines how up-to-date the data in the ADS must be. There are two main aspects of a data freshness service level: (1) how often is the data in the ADS updated, and (2) how long after the data is updated will it be accessible.
<ul style="list-style-type: none">▪ Query Performance service levels are generally focused on response time. However, it is also critical to consider the throughput requirements of the environment to define the number of concurrent queries to be supported.<ul style="list-style-type: none">▪ Distinct classes of workload defined by query complexity and priority should be established with individual service level agreements for each.▪ Query prioritization can be used to allocate resources so that some queries are impacted less by concurrent workloads than others.▪ Service levels may also be defined differently for distinct times of day.
Physical and System Security
<ul style="list-style-type: none">▪ Implement appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of Institutional Data.
<ul style="list-style-type: none">▪ Ensure that data is assigned an appropriate classification.
<ul style="list-style-type: none">▪ Ensure that systems containing sensitive information are physically secured from unauthorized access.
<ul style="list-style-type: none">▪ Ensure that actual or suspected data security breaches, especially when involving sensitive data, are reported immediately and that any recommended corrective action is implemented.
<ul style="list-style-type: none">▪ Ensure that procedures are followed to mitigate all identified compromises or identified data security threats.
Data Quality Standards
<ul style="list-style-type: none">▪ Ensure that each data element has adequate documentation on appropriate usage and notes.
<ul style="list-style-type: none">▪ Document the origin and sources of authority on each metadata element.
Disaster Recovery Plans
<ul style="list-style-type: none">▪ Ensure that risk assessments are performed (including disaster recovery plans, backup and contingency plans) as required, including those required by HIPAA for all PII. Risk assessment is recommended for all other sensitive or mission critical data.
<ul style="list-style-type: none">▪ Establish an ongoing process to ensure that the necessary steps are taken to:<ul style="list-style-type: none">▪ Identify the impact of potential losses.▪ Maintain viable recovery strategies and plans.▪ Ensure the continuity of operations through personnel training, plan testing, and maintenance.

The categories/types of data required to perform SC missions, the organizations that produce those types of data, and the systems/tools those organizations use to provide their data are analyzed in Appendix C. Producers of SC data include DoD, non-DoD Federal government, non-US (multinational and coalition), and non-governmental organizations.

Appendix A – Source Documents for Requirements

US Pacific Command, TSCMIS Process Document, updated 13 July 2009
US Joint Forces Command J9, Memorandum for Record, Cooperative Security (CS) Experiment Recommendations for Global Theater Security Cooperation Management Information System (G-TSCMIS), 15 September 2009
US Central Command TSCMIS Users' Guide, Web-Based Version 3, February 2007
Strategy Division – Office of Plans, Defense Security Cooperation Agency, Standardizing Security Cooperation Assessment Inputs, Task 2 Report, 18 April 2007 (S)
Strategy Division – Office of Plans, Defense Security Cooperation Agency, Standardizing Security Cooperation Assessment Inputs, Task 3 Report, 6 June 2007
US Joint Forces Command Cooperative Security Experiment Series Recommendations and Synthesis (R&S) Conference Final Report, 9 September 2009
Headquarters Department of the Army, Army Global Outlook System (ARGOS) User's Guide, May 2009
US Special Operations Command, Memorandum for the Chairman Joint Chiefs of Staff, US Special Operations Command Addendum to the FY 2010-2015 Integrated Priority List, 28 February 2008

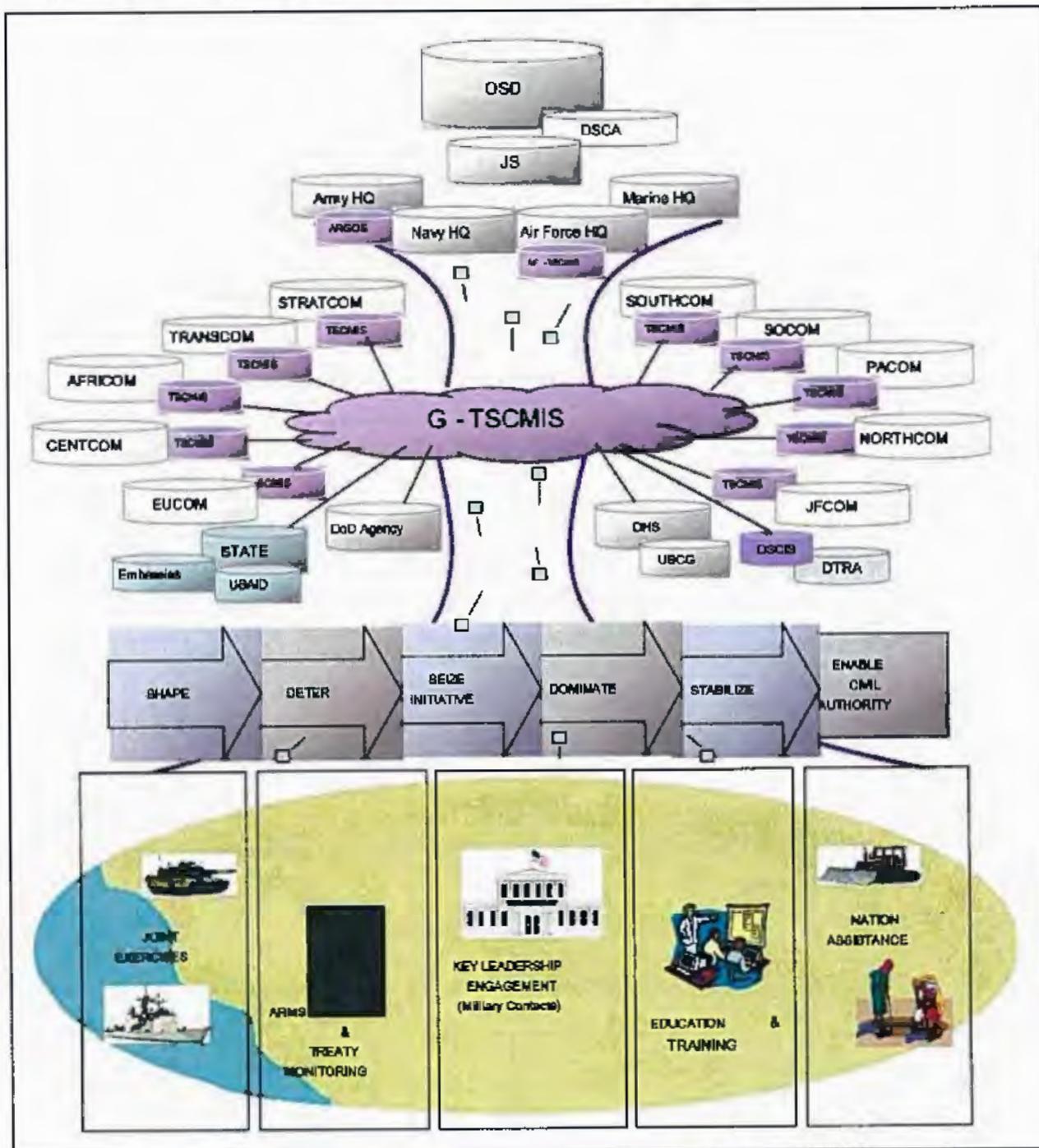
Draft/Pre-Decisional Documents

Global-Theater Security Cooperation Management Information System (G-TSCMIS) Roadmap, Version 1.0, 5 March 2009, (Pre-decisional draft)
Defense Security Cooperation Agency (DSCA), Global TSCMIS Data Integration and Display Capability & Transition Planning Document, 30 September 2008 (Draft)
Transnational Information Sharing Cooperation (TISC) Joint Capability Technology Demonstration (JCTD), "A Roadmap to an Operationally Validated Concept of Operations (CONOPS) for Stability, Security, Transition, and Reconstruction (SSTR) and Theater Security Cooperation (TSC) Operations Using TISC Enabling Capabilities," Vers 1.0, August 2009 (Draft)

(INTENTIONALLY BLANK)

A-2

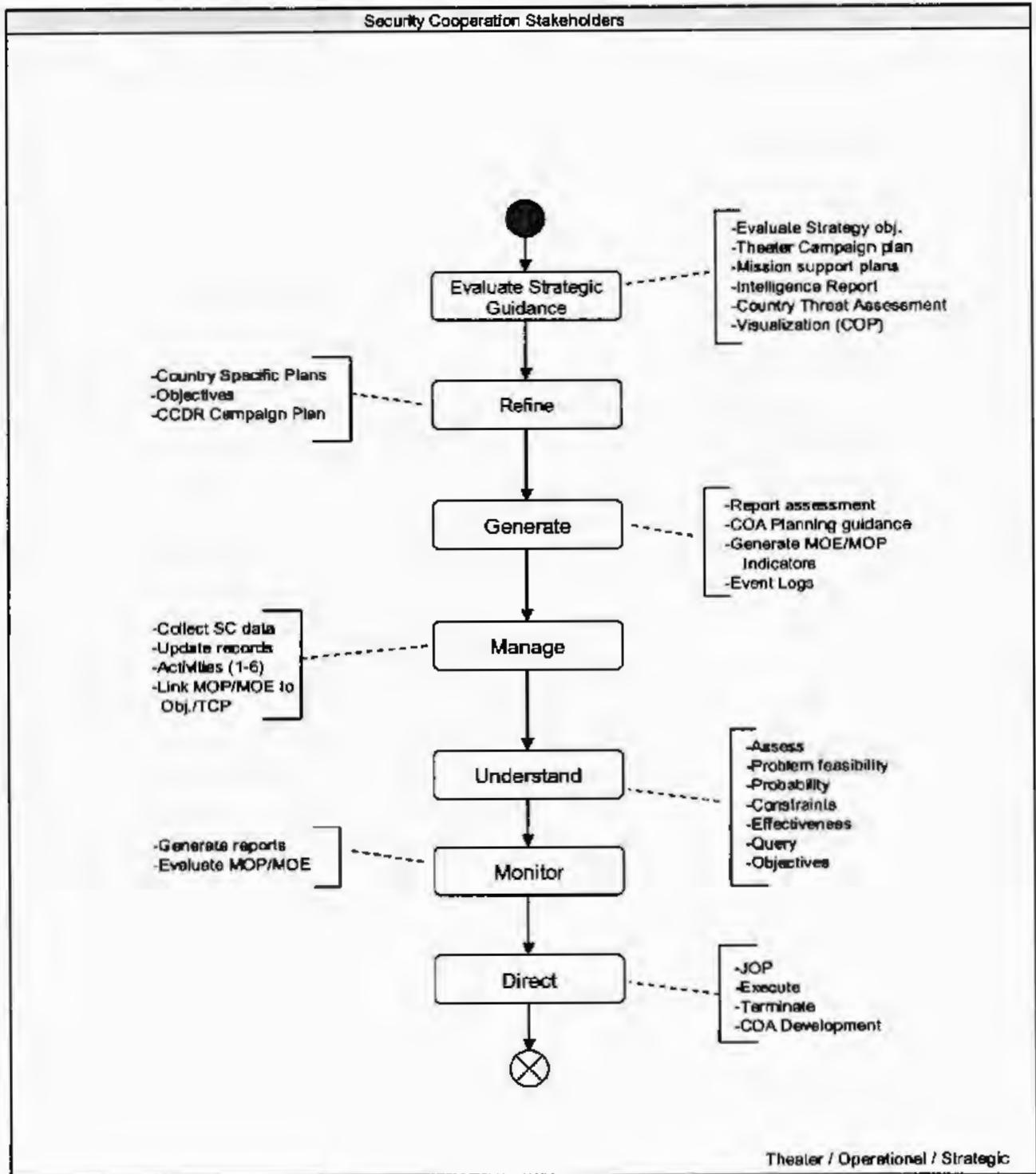
Appendix B – Operational Views/Activity Models



OV1, High Level Operational Concept Graphic

Figure 2: OSD/Joint Staff - Security Cooperation (SC)

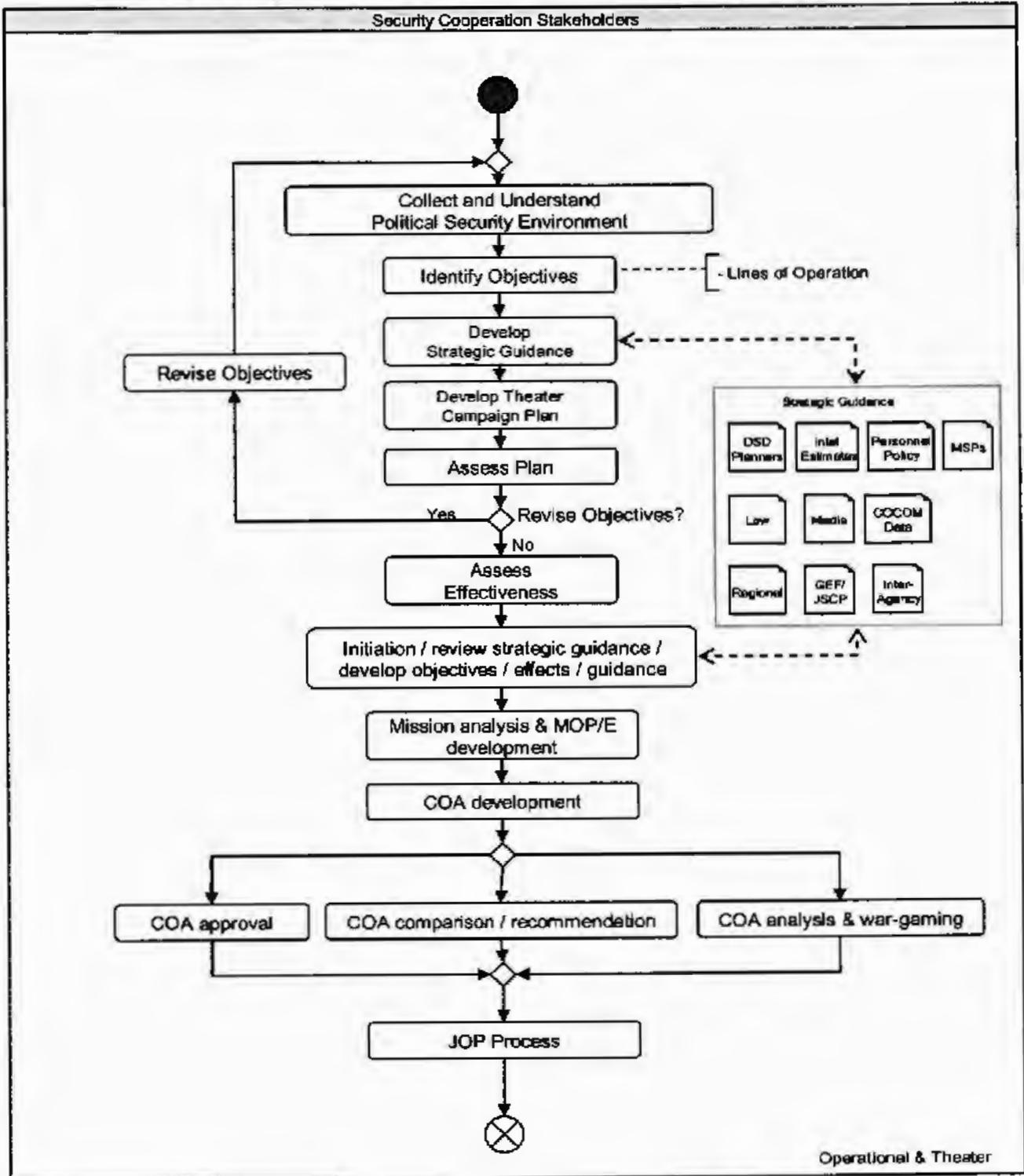
Assess, Report & Monitor Security Cooperation



OV-5b, Operational Activity Model

Figure 3: Assess, Report and Monitor SC

Develop Concept for Security Cooperation

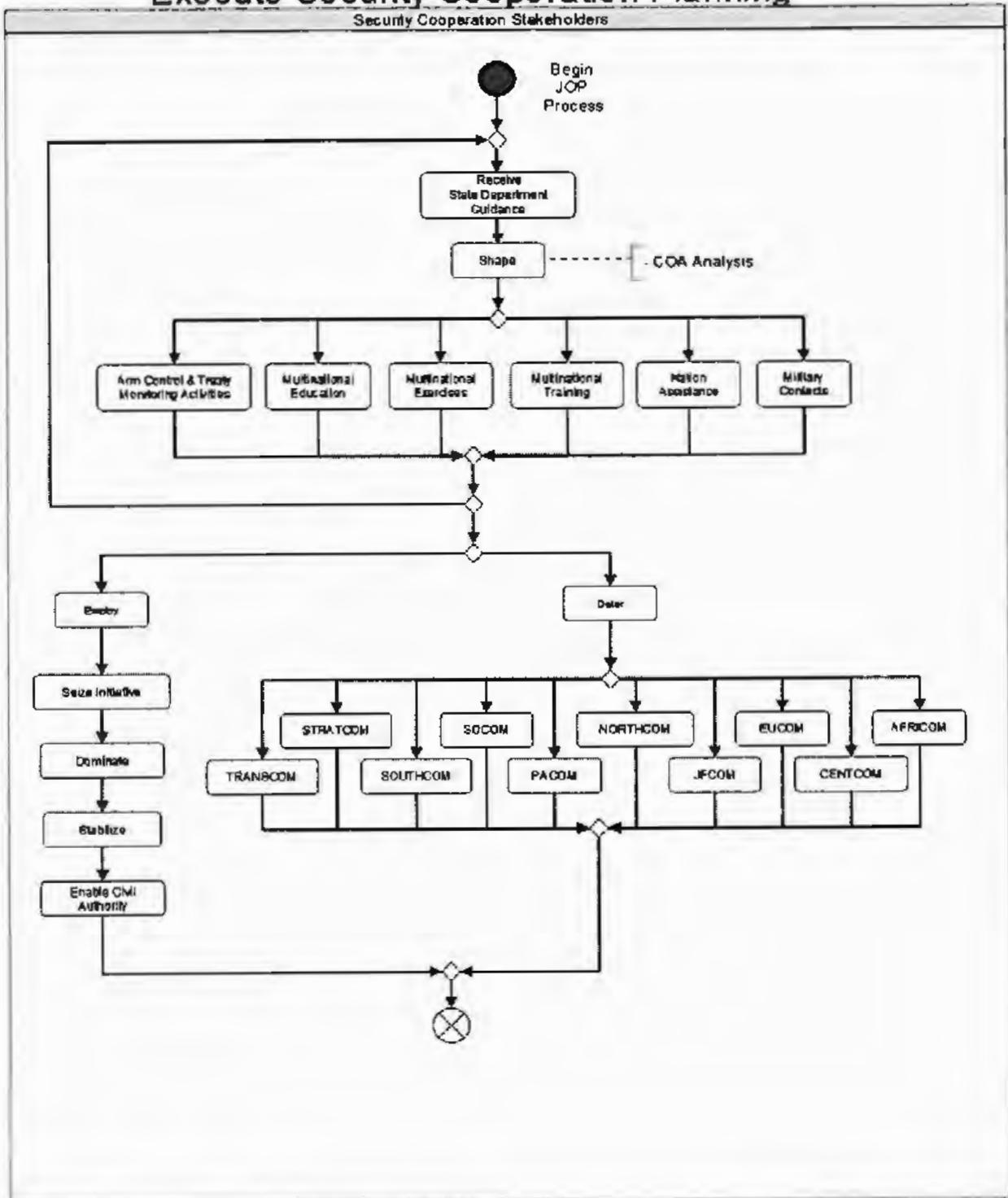


OV-5b, Operational Activity Model

Figure 4: Develop Concept for SC

B-3

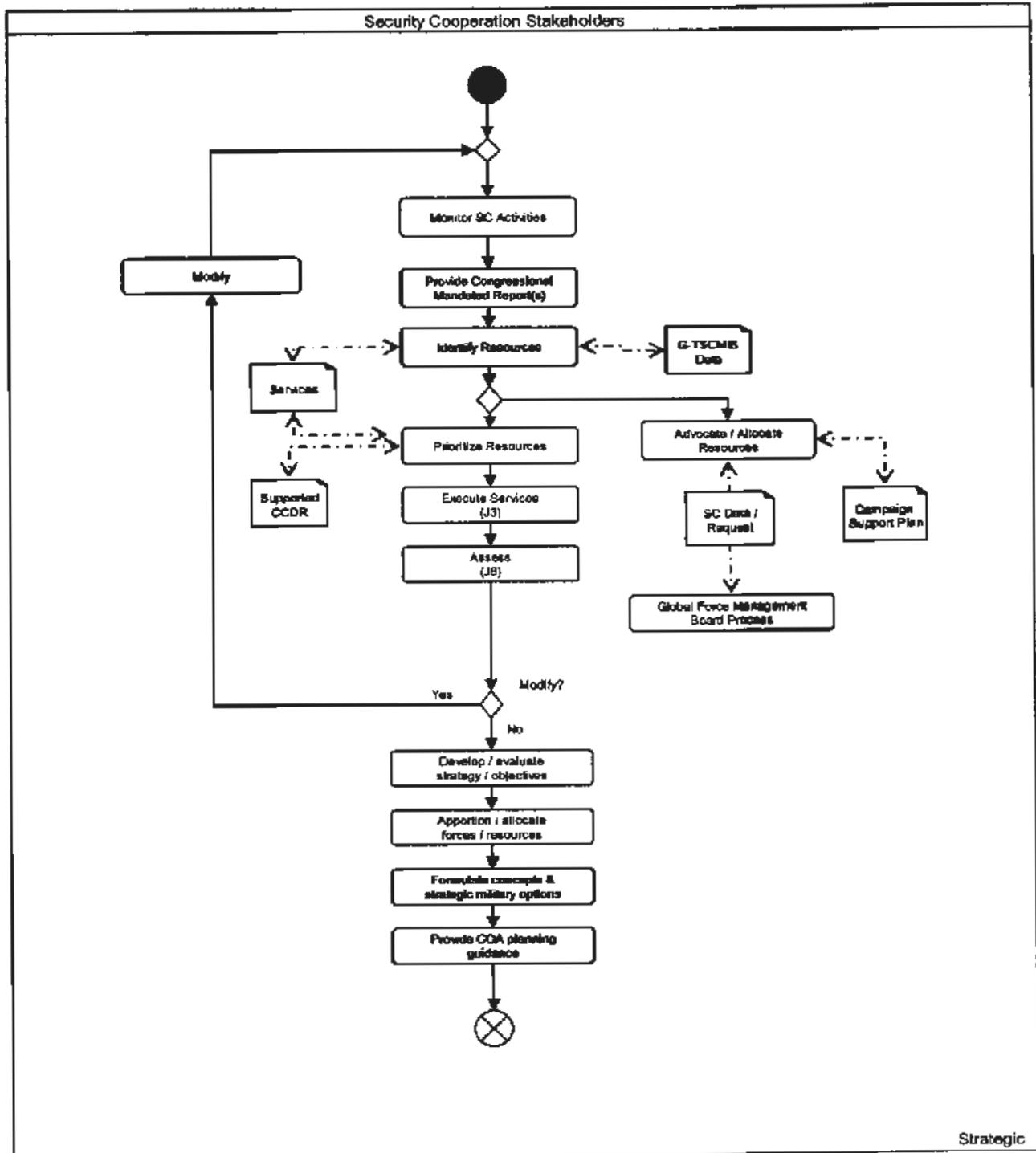
Execute Security Cooperation Planning



OV-5b, Operational Activity Model

Figure 5: Execute SC Planning

OSD Joint Staff - Security Cooperation



OV-5b, Operational Activity Model

Figure 6: OSD Joint Staff – SC

(INTENTIONALLY BLANK)

B-6

Appendix C– Security Cooperation Authoritative Data Sources (ADS)

Security Cooperation ADS Analysis

C2 CPM approach to identifying ADS is a repeatable approach, not specific to the C2 Portfolio, that identifies the types of information needed to perform a specific mission, what organizations are responsible for providing that type of data, and how those organizations provide their data.

1) Identify the SC data needs (types of data required to perform SC missions). The SC community needs both current and historical data on SC Planning (Strategy/Campaign/Activity/Event/Resources), SC Execution, and Assessment. The SC community divides their data into 15 broad categories:

Table 4: Security Cooperation Information Needs

<ul style="list-style-type: none"> • Counter/Non-Proliferation <ul style="list-style-type: none"> • Consequence Management Programs • Cooperative Threat Reduction Program • Nonproliferation/Counterproliferation Programs • Treaty Compliance Activities • Research and Development Activities 	<ul style="list-style-type: none"> • Multinational Education <ul style="list-style-type: none"> • Defense Institute for Medical Operations • Regional Strategic Studies Academic Programs • Senior/Intermediate Service Schools
<ul style="list-style-type: none"> • Counter Narcotics Assistance <ul style="list-style-type: none"> • Counter Drug and Counter Narcoterrorism support 	<ul style="list-style-type: none"> • Multinational Exercises <ul style="list-style-type: none"> • Bilateral/Multilateral Exercises • Exercise-Related Construction
<ul style="list-style-type: none"> • Defense & Military Contacts <ul style="list-style-type: none"> • Conferences/seminars/staff-to-staff events • Exchange Programs (Small unit / individual) • Official Visits • Port Visits/Ship Rider/Distinguished Visitor (DV) Embarks Programs • State Partnership Programs • Chaplain Program • Joint Contact Team Program • Military HIV/AIDS Prevention Program 	<ul style="list-style-type: none"> • Multinational Training <ul style="list-style-type: none"> • Counter-narcotics Training • Joint Combined Exchange Training • Maritime Law Enforcement, Safety, and Security Training • Mobile Training Teams (MTT) • Regional Training Events • US Coast Guard (USCG) Education & Training
<ul style="list-style-type: none"> • Defense Support to Public Diplomacy 	<ul style="list-style-type: none"> • Multinational Experimentation <ul style="list-style-type: none"> • Technical Cooperation Program (TCP)

<ul style="list-style-type: none"> • Humanitarian Assistance (HA) <ul style="list-style-type: none"> • HA Program-Excess Property • HA Program-Other (contracts between DoD & local laborers to construct/renovate public facilities; disaster management training) • Humanitarian Civic Assistance Program • Humanitarian Mine Action • Overseas Humanitarian Disaster & Civic Aid (OHDACA) 	<ul style="list-style-type: none"> • Security Assistance <ul style="list-style-type: none"> • Combating Terrorism Fellowship Program • Excess Defense Articles • Health Security Cooperation • Direct Commercial Contracts • Peacekeeping Operations • Foreign Military Finance Grants • Foreign Military Sales • International Military Education & Training (IMET)
<ul style="list-style-type: none"> • Information Operations <ul style="list-style-type: none"> • Combat Camera • Military Information Support Team 	<ul style="list-style-type: none"> • Operational Activities
<ul style="list-style-type: none"> • Information Sharing/Intelligence Cooperation <ul style="list-style-type: none"> • Intelligence Exchanges 	<ul style="list-style-type: none"> • Other Security Cooperation Activities <ul style="list-style-type: none"> • Arms Control & Treaty Verification • C4I Interoperability Initiatives • Defense Environmental Security International Cooperation • Small Arms & Light Weapons (SALW)
<ul style="list-style-type: none"> • International Armaments Cooperation 	

2) Map SC data needs (from a producer perspective) against candidate ADS. The C2 CPM considers an ADS to be a combination of:

- Operational nodes/data owners/data producers. The operational node/data owner/data producer is an entity/organization with the authority and responsibility to provide specified Authoritative Data, making it visible, accessible, understandable, and trustable.
- Systems & tools data producers use to provide their data. The systems/tools used by the data producers to provide their data can be an application/automated information system, a web service, a database, a data feed, a data store/data cache, an unstructured/semi-structured file, or a social networking method (e.g., chat).
- Databases/data stores that feed the systems/tools. Data stores/data feeds/databases that do not make their data directly available through web/data services but provide Authoritative Data to the systems/tools.

a) Operational nodes/data owners/data producers. The organizations responsible for producing SC data include:

Table 5: Security Cooperation Data Producers

<ul style="list-style-type: none"> • Combatant Commands <ul style="list-style-type: none"> • Geographic <ul style="list-style-type: none"> - AFRICOM / CENTCOM / EUCOM / NORTHCOM / PACOM / SOUTHCOM <ul style="list-style-type: none"> • J5 – Event Plans • J3 – Execution • J8 – Assessment • J2 – Intelligence Exchanges • J7 – Exercises • Functional <ul style="list-style-type: none"> - STRATCOM - TRANSCOM - JFCOM - SOCOM/J35/J33
<ul style="list-style-type: none"> • Services <ul style="list-style-type: none"> • Navy <ul style="list-style-type: none"> - Navy International Programs Office (NIPO) – SA Policy; Principal agent for SA matters - Navy Inventory Control Point (NICP) International Programs Directorate – foreign requisitions for SA - Navy Education & Training SA Field Activity (NETSAFA) – Navy SA Training Program - Navy Education & Training Command (NETC) – International participation in PME Programs - Navy International Engagement Division (OPNAV N52) – Humanitarian Civil Assistance (HCA)/Theater Security Cooperation (TSC)/International Relations - Lessons Learned System • Marine Corps <ul style="list-style-type: none"> - HQMC International Issues Branch, SC/SA Policy & regional desk officers - MARCORSSYSCOM International Programs – SA acquisition & logistics matters; FMS - Training & Education Command (TECOM) – International Training & Education <ul style="list-style-type: none"> • USMC Security Cooperation Education & Training Center (SCETC) - Lessons Learned System • Air Force <ul style="list-style-type: none"> - Secretary of the Air Force for International Affairs (SAF/IA) <ul style="list-style-type: none"> • SAF/IAPA – International Airmen Division (exchange programs) • SAF/IAPQ – Armaments Cooperation Division • SAF/IAPX – Security Assistance Policy and International Training and Education Division - Air Force Security Assistance Center (AFSAC) - Air Education & Training Command (AETC) <ul style="list-style-type: none"> • AETC/IA – International participation in PME Programs • Air Force Security Assistance Training Squadron (AFSAT) - AF/A5 • Army <ul style="list-style-type: none"> - HQDA/G35 Army International Affairs - Assistant Secretary of the Army (Acquisition, Logistics & Technology) – ASA(ALT) <ul style="list-style-type: none"> • Deputy Ass't Secretary of the Army (Defense Exports and Cooperation Div.) - Army Materiel Command (AMC) <ul style="list-style-type: none"> • US Army Security Assistance Command (USASAC) • Research Development and Engineering Command (RDECOM) - Training and Doctrine (TRADOC) Command <ul style="list-style-type: none"> • Security Assistance Training Field Activity (SATFA) • Security Assistance Training Management Organization (SATMO) - Corps of Engineers (COE)

<ul style="list-style-type: none"> • National Guard Bureau International Affairs (NGB-IA)
<ul style="list-style-type: none"> • Coast Guard <ul style="list-style-type: none"> – Director of International Affairs & Foreign Policy – International Training Division, USCG Training Center Yorktown
<ul style="list-style-type: none"> ▪ Defense Threat Reduction Agency (DTRA) <ul style="list-style-type: none"> • Cooperative Threat Reduction (CTR) Directorate (OP-CT) • Onsite Inspection (OP-OS) Directorate • Combat Support (OP-CS) Directorate • Plans and Doctrine Integration Division (CW-PDI) • Research and Development Enterprise (ADRD) • Advanced Systems and Concepts Office (DIR-AS)
<ul style="list-style-type: none"> ▪ OSD <ul style="list-style-type: none"> • OSD/Policy <ul style="list-style-type: none"> – Global Strategic Affairs – Regional International Security Affairs Offices – DSCA – Defense Security Cooperation Agency <ul style="list-style-type: none"> • Defense Security Assistance Development Center (DSADC) • Defense Institute of Security Assistance Management (DISAM) • Global Center for Security Cooperation • Strategy Directorate (Strategy/Assessments/Policy) • Operations Directorate (Policy/Planning/Execution of Country programs) • Programs Directorate (IMET/FMF/HA/Disaster Relief/Demining) DTSA – Defense Technology Security Administration <ul style="list-style-type: none"> • International Security Division • OSD(AT&L) Director, International Cooperation • OSD/Comptroller (SA Policy & Procedures Financial management regulations)
<ul style="list-style-type: none"> ▪ Joint Staff <ul style="list-style-type: none"> • JS/J7 • Joint Center for International Security Force Assistance (JCISFA)
<ul style="list-style-type: none"> ▪ State Department (DoS) <ul style="list-style-type: none"> • Under Secretary for Political Affairs <ul style="list-style-type: none"> Six geographic bureaus Bureau of International Narcotics and Law Enforcement Affairs – counter-narcotics training & programs Bureau of International Organization Affairs – peacekeeping, humanitarian assistance • Coordinator for Counterterrorism • Coordinator for Reconstruction & Stabilization – stabilize & reconstruct societies in transition from conflict • Bureau of Diplomatic Security – Antiterrorism Assistance Program training • Directorate of Defense Trade Controls • Under Secretary for Arms Control and International Security <ul style="list-style-type: none"> – Bureau of Political-Military Affairs —principal link between DoS & DoD for FA: security assistance training; demining (FMF, IMET, PKO); Directorate of Defense Trade Controls – Bureau of International Security and Nonproliferation – nonproliferation & arms control; prevent/protect/respond to WMDs – Bureau for Verification & Compliance – treaty compliance policy & implementation • International Communications and Information Policy Group – interoperability • Under Secretary for Democracy and Global Affairs <ul style="list-style-type: none"> – Bureau of Population, Refugees, and Migration – refugee assistance programs • Millennium Challenge Corporation (U.S. government corporation created to reduce poverty through sustainable economic growth)

<ul style="list-style-type: none"> ▪ USAID <ul style="list-style-type: none"> • Director of Foreign Assistance – economic, technical, and humanitarian assistance programs for sustainable development; foreign students at American colleges • Regional Bureaus • Bureau of Democracy, Conflict, and Humanitarian Assistance • Bureau for Foreign Assistance <ul style="list-style-type: none"> – Office of US Foreign Disaster Assistance
<ul style="list-style-type: none"> ▪ DHS <ul style="list-style-type: none"> • Policy Office of International Affairs • Office of Counternarcotics Enforcement • FEMA <p style="text-align: center;">Office of External Affairs International Affairs Organization</p>
<ul style="list-style-type: none"> ▪ DoJ <ul style="list-style-type: none"> • ATF • DEA • FBI
<ul style="list-style-type: none"> ▪ Agriculture Dept <ul style="list-style-type: none"> • Foreign Agricultural Service
<ul style="list-style-type: none"> ▪ Commerce Dept <ul style="list-style-type: none"> • Bureau of Industry and Security
<ul style="list-style-type: none"> ▪ Treasury Dept <ul style="list-style-type: none"> • Office of International Affairs • Office of Foreign Assets Control • Office of Technical Assistance • Office of Terrorism and Financial Intelligence
<ul style="list-style-type: none"> ▪ FDA HHS <ul style="list-style-type: none"> • National Institutes of Health • Office of Global Health Affairs • Office of International Programs
<ul style="list-style-type: none"> ▪ Red Cross <ul style="list-style-type: none"> • International Services
<ul style="list-style-type: none"> ▪ United Nations <ul style="list-style-type: none"> • Office for the Coordination of Humanitarian Affairs
<ul style="list-style-type: none"> ▪ Humanitarian Demining Information Center – James Madison University (JMU)

b) Systems/tools data producers use to provide their data and data stores/databases that feed the systems/tools (with links where available):

Table 6: Systems/Tools used by Security Cooperation Data Producers

<ul style="list-style-type: none"> • Combatant Commands <ul style="list-style-type: none"> - Theater Security Cooperation Strategy/Plan (TSCS/TSCP) - Theater Campaign Plan (TCP) - Combined Education & Training Program Plan (CETPP) - Country Campaign Plan - Country Security Cooperation Plan - Objectives & Desired Effects Assessments - Monthly Country Reports - TSCMIS <ul style="list-style-type: none"> • PACOM TSCMIS Portal (SIPR) (http://www.hq.pacom.smil.mil/j5/j56/) • PACOM TSCMIS Login (SIPR) (http://www2.hq.pacom.smil.mil/tepmis) • EUCOM <ul style="list-style-type: none"> • EUCOM TSCMIS Portal (SIPR) (http://scw1.eucom.smil.mil/TSCMIS_EU/Portals/AgencyPortals) • EUCOM TSCMIS login (SIPR) (http://scw1.eucom.smil.mil/tscmis_eu) • AFRICOM <ul style="list-style-type: none"> • AFRICOM TSCMIS Portal (SIPR) (http://scw1.eucom.smil.mil/TSCMIS_AF/Portals/AgencyPortals) • AFRICOM TSCMIS login (SIPR) (http://scw1.eucom.smil.mil/tscmis_af) • CENTCOM TSCMIS Portal (SIPR) (http://hqsdb05.centcom.smil.mil/Tscmis2/SystemSpecific/CountryPortalListing.aspx) • SOUTHCOM Country Portals (SIPR) (http://scportalanon.hq.southcom.smil.mil/Countries/default.aspx) <ul style="list-style-type: none"> • TSCMIS tab on country pages • NORTHCOM TSCMIS Portal (SIPR) (http://demeter.hq.pacom.smil.mil/Tscmis2_Northcom/app/module/overviews/Agency/Overview.aspx?SID=&Agency=ARNORTH&FY=2008) • SOCOM Security Cooperation Portal (SIPR) (http://public.opb.socom.smil.mil/sites/ope_us/TSC/default.aspx) • ARMY <ul style="list-style-type: none"> • ARMY ARGOS (TSCMIS) Portal (SIPR) (http://www.hqda-q3.army.smil.mil/ARGOS/Portals/DAMO-SSI/Default.asp?tab=2) • ARMY ARGOS (TSCMIS) login (SIPR) (http://www.hqda-q3.army.smil.mil/ARGOS) • DTRA <ul style="list-style-type: none"> • DTRA Security Cooperation Information System (DSCIS) - Theater Operational Planning and Assessment Service (TOPAS) (SIPRNET/JWICS) - Joint Capabilities Requirements Manager (JCRM) - Concept Funding Request (CFR) Database
<ul style="list-style-type: none"> • DoD Security Cooperation wiki/Portal (SIPR) (http://www.intelink.sgov.gov/wiki/Portal:DoD_Security_Cooperation) <ul style="list-style-type: none"> - Links to EC Portals, Theater/Campaign/Campaign Support Plans
<ul style="list-style-type: none"> • Global TSCMIS wiki/Portal (SIPRNET) (http://www.intelink.sgov.gov/wiki/Global_TSCMIS_Initiative)
<ul style="list-style-type: none"> • JS/J7 <ul style="list-style-type: none"> - Joint Training Information Management System (JTIMS) (http://jtims.drc.com/jtims_rmmf/index.jsp) <ul style="list-style-type: none"> • JTIMS Login (http://jtims.drc.com/jtims_rmmf/login.do)

<ul style="list-style-type: none"> • DSCA <ul style="list-style-type: none"> - Security Assistance Network (SAN) (https://www.idss.ida.org/san/login.prg) <ul style="list-style-type: none"> • Training Management System (available through SAN) (http://www.disam.dsca.mil/itm/Automation/TMS7FAQS.asp) • Security Cooperation Organizations-Training Web (SCO-TWeb) -- Link provides access information (http://www.disam.dsca.mil/itm/automation/SAOWeb.asp) • IMSO Web (International Military Student Officer) (http://www.disam.dsca.mil/itm/automation/IMSOWeb.asp) - International Security Assistance Network (https://www.idss.ida.org/isan/login.prg) - Defense Security Assistance Management System (DSAMS) (https://dsams.dsca.mil/logon/logo.asp) - Security Assistance Budget Web Tool (FMF & IMET) - includes link to request account (https://www.fmfimet.net/Site/LogIn.aspx) - Overseas Humanitarian Assistance Shared Information System (OHASIS) (https://www.ohasis.org/OHASIS/Login.aspx) - Partnership for Peace Information Management System (PIMS) Portal (http://www.pims.org/) <ul style="list-style-type: none"> • PIMS Login Page (https://members.pims.org/user) - Regional International Outreach (RIO) Collaboration Network access through the Global Center for Security Cooperation (GCSC) (https://gcsc.rio-net.org/) - Security Cooperation Information Portal (SCIP) (https://www.scportal.us/home/) - Security Assistance Automated Resource Management System (SAARMS) <ul style="list-style-type: none"> • Budget/execution – stand-alone PC software, uploads into SAN using Integrated SAARM (ISAARM)
<ul style="list-style-type: none"> • Services <ul style="list-style-type: none"> - Air Force <ul style="list-style-type: none"> • Air Force Security Assistance Center (AFSAC) Online (https://afsac.wpafb.af.mil/) • AFSAC Security Assistance Manpower Resource System (https://www.my.af.mil/samrs/) • Air Force Security Assistance Management Information System (SAMIS) (through DISA's Multi-host Internet Access Portal (MIAP)) (https://miap.csd.disa.mil/) - Army <ul style="list-style-type: none"> • Army Security Assistance Command (https://usasac.army.mil/) • Army Training Information Management System (ARTIMS) (https://artims.forscom.army.mil/) • Army Export Control System Electronic Performance Support System (EPSS) Portal (http://www.usasac.army.mil/EPSS/Start.htm) • US Army Corps of Engineers (USACE) MOA Database Portal (http://www.usace.army.mil/CEMP/iis/Pages/MOADatabase.aspx) • Acquisition Technology (https://stem-collabsuite.altess.army.mil) - Navy <ul style="list-style-type: none"> • Navy Inventory Control Point (NICP) International Programs Directorate Asset Visibility System (https://nicppla11.navsysa.navy.mil/assetviz/Index.aspx?Banner=ON) • InRelief.org Humanitarian Assistance Portal (http://partnerpage.google.com/inrelief.org) • U.S. Navy International Training & Education Catalog (https://www.netsafa.navy.mil/Navv_Training_Catalog_2009.pdf) - Marine Corps <ul style="list-style-type: none"> • USMC Force Synchronization Playbook • SCETC's Security Cooperation Office Desktop Guide • Mobile Training Team Catalog • International Military Student Officer (IMSO) Guide

<ul style="list-style-type: none"> - Coast Guard <ul style="list-style-type: none"> • <i>USCG International Training Handbook</i> (http://www.uscg.mil/international/docs/ITH12.1.pdf) • <i>International Mobile Training & Education Catalog</i> (http://www.uscg.mil/tcyorktown/international/itd/Docs/2005%20BROCHURE_Final.zip) • <i>International Port Security Program Portal</i> (Login at upper right, IPS Program link at upper right under Featured Homeport Links) (http://homeport.uscg.mil/mycg/portal/ep/home.do)
<ul style="list-style-type: none"> - National Guard Bureau <ul style="list-style-type: none"> • <i>State Partnership Program Part I Doctrine & Development/Initial Procedures</i> (https://www.us.army.mil/suite/doc/14755505) • <i>State Partnership Program Part II SPP Management</i> (https://www.us.army.mil/suite/doc/14755506)
<ul style="list-style-type: none"> • OSD <ul style="list-style-type: none"> - <i>DoD Humanitarian Assistance Program - Internet (HAP-I)</i> (http://dentonfunded.ohasis.org/Logon.asp?Mode=Enter) - <i>DoD Financial Management Regulation 7000.14-R Ch 15 Security Assistance Policy and Procedures</i> (http://www.defenselink.mil/comptroller/fmr/15/index.html) - <i>DTSA Export License Status Advisor (ELISA)</i> (http://elisa.osd.mil/)
<ul style="list-style-type: none"> • DTRA <ul style="list-style-type: none"> - <i>Security Cooperation Activity Plan</i> http://ocweb.osn.dtra.smil.mil/Documents/cfDocsTmp/cwip_dod_tsc_5-27/docc_6-4617/Regional%20Combating%20WMD%20Strategy_Security%20Cooperation%20Activi.pdf - <i>DTRA Security Cooperation Information System</i>
<ul style="list-style-type: none"> • <i>USJFCOM HarmonieWeb Humanitarian Assistance Portal</i> (http://www.harmonieweb.org/Pages/Default.aspx)
<ul style="list-style-type: none"> • DoS <ul style="list-style-type: none"> - <i>Foreign Assistance Coordination and Tracking System (FACTS) II</i> (http://usqfacts.net/Login/Login.aspx) - <i>USAID HIV/AIDS Surveillance Database</i> (http://hivaidsurveillancedb.org/hivdb/StartPage.aspx) - <i>World Health Organization/USAID International Emergency Event Database</i> (http://www.emdat.be/Database/terms.html) - <i>Abuse Case Evaluation System (ACES)</i> (http://aces.state.gov/) - <i>Foreign Assistance Standardized Program Structure and Definitions - 12 Dec 2008</i> (http://www.state.gov/documents/organization/115258.pdf) - <i>Standard Foreign Assistance Indicators (potential assessment categories)</i> (http://www.state.gov/f/indicators/index.htm) <ul style="list-style-type: none"> • <i>Master List of Standard Indicators</i> (http://www.state.gov/documents/organization/115255.pdf) • <i>Indicator Handbooks (links are on Indicators web page)</i>
<ul style="list-style-type: none"> • <i>Agriculture Department Export Sales Query System</i> (http://www.fas.usda.gov/esquery/esrq.aspx)
<ul style="list-style-type: none"> • <i>FEMA International Coordination Support Annex</i> (http://www.fema.gov/pdf/emergency/nrf/nrf-support-international.pdf)
<ul style="list-style-type: none"> • <i>Commerce Department Export Control Automated Support System-Redesign (ECASS-R) Simplified Network Access Process-Redesign (SNAP-R)</i> (https://snapr.bis.doc.gov/snapr/)

- **United Nations**
 - United Nations UNdata Database (<http://data.un.org/>)
 - United Nations Portal for Humanitarian Affairs (<http://www.un.org/en/humanitarian/>)
 - ReliefWeb (<http://www.reliefweb.int/rw/dbc.nsf/doc100?OpenForm>)
 - Integrated Regional Information Networks (IRIN) (<http://www.irinnews.org/>)
 - Humanitarian Information Centers Portal (<http://www.humanitarianinfo.org/>)
 - Global Disaster Alert and Coordination System (GDACS) Virtual Onsite Operations Coordination Center (VOOCC) login page (<http://ocha.unog.ch/virtualosccc/>)
 - OneResponse Humanitarian Information Toolbox login page (<http://onerresponse.info/Pages/default.aspx>)
 - Who/What/Where Contact Management Directory (<http://3w.unocha.org/WhoWhatWhere/>)
- American Red Cross International Services Resource Portal (including regional strategic planning /country annual planning tools/templates and capacity building guidance to help *design/implement/assess country programs*) (<http://www.redcross.org/portal/site/en/menuitem.53fabf6cc033f17a2b1ecbf43181aa0/?vqnextoid=0fb59891353ab110VgnVCM10000089f0870aRCRD&currPage=92879891353ab110VgnVCM10000089f0870aRCRD>)

(INTENTIONALLY BLANK)

C-10

Appendix D – Definitions and Acronyms

D.1 Definition List

Adaptive Planning and Execution (APEX) — Department level system of joint policies, processes, procedures and reporting structure, supported by communications and information technology that is used by the Joint Planning and Execution Community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. Governs the planning and execution of joint operations consistent with the Adaptive Planning (AP) vision. These department level policies and procedures will be documents in CJCSMs and will constitute the successor to the Joint Operation Planning and Execution CJCSMs currently in effect. (AP RM II, AP CONOPS)

Assessment — 1. A continuous process that measures the overall effectiveness of employing joint force capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating an effect, or achieving an objective. 3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or “agents.” (JP 1-02; source, JP 3-0)

Capability Development Document (CDD) — A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability. The CDD may define multiple increments if there is sufficient definition of the performance attributes (key performance parameters, key system attributes, and other attributes) to allow approval of multiple increments. (CJCSI 3170.01G)

Capability Definition Package (CDP) — The CDP is a tailored Joint Combat Capability Developer (JCCD) product which refines the Capability Development Document (CDD) into a set of synergistic units (packages). It provides the operational perspective, functional behavior, and performance details needed to translate warfighter capabilities into acquisition and engineering terminology for materiel solution development. (Joint Combat Capability Developer (JCCD) Management Plan)

Common Operational Picture (COP) — A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 1-02; source, JP 3-0)

End State — The set of required conditions that defines achievement of the commander’s objectives. (JP 1-02; source, JP 3-0)

Interagency — United States Government agencies and departments, including the Department of Defense. See also interagency coordination. (JP 1-02; source, JP 3-08)

Interagency Coordination — Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies for the purpose of achieving an objective. (JP 1-02; source, JP 3-0)

Joint Operation Planning Process — An orderly, analytical process that consists of a logical set of steps to analyze a mission; develop, analyze, and compare alternative courses of action against criteria of success and each other; select the best course of action; and produce a joint operation plan or order. Also called JOPP. (JP 1-02; source, JP 5-0)

Line of Operations — 1. A logical line that connects actions on nodes and/or decisive points related in time and purpose with an objective(s). 2. A physical line that defines the interior or exterior orientation of the force in relation to the enemy or that connects actions on nodes and/or decisive points related in time and space to an objective(s). Also called LOO. (JP 1-02; source, JP 3-0)

Link — (DOD only) A behavioral, physical, or functional relationship between nodes. (JP 1-02; source, JP 3-0)

Non-Governmental Organization (NGO) — A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02; source, JP 3-08)

Situational Awareness (SA) — Fused battlespace awareness tailored to provide current and projected disposition of hostile, neutral, and friendly forces through near real time/real time sensor data and Service/National/inter-Agency/joint-provided data sources. (CDD definition, Annex C)

Security Cooperation (SC) — All Department of Defense interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation. (JP1-02)

Security Cooperation Planning — The subset of joint strategic planning conducted to support the Department of Defense's security cooperation program. This planning supports a combatant commander's theater strategy. (JP 1-02; source, JP 5-0)

Security Force Assistance (SFA) — Described as that set of activities that contribute to the development of capability and capacity of foreign security forces (FSF) and their supporting institutions.

Theater Campaign Plans — Plans developed by geographic combatant commands that focus on the command's steady-state activities, which include operations, security cooperation, and other activities designed to achieve theater strategic end states. It is incumbent upon geographic Combatant Commanders to ensure any supporting campaign plans address objectives in the GEF global planning effort and their respective theater campaign plans. Contingency plans for responding to crisis scenarios are treated as branch plans to the campaign plan. (DoDD 5132.03)

D.2 Acronym List

ABAC	Attribute Based Access Control
ADS	Authoritative Data Sources
AMC	Army Materiel Command
AO	Area of Operations
AOR	Area of Responsibility
APEX	Adaptive Planning and Execution
ARGOS	Army Global Outlook System
ATF	Alcohol, Tobacco, and Firearms
AT&L	Acquisition, Technology, and Logistics
BPM	Business Process Model
C2	Command and Control
CCDR	Combatant Commander
CDD	Capability Development Document
CDP	Capability Definition Package
CDS	Cross Domain Solutions
CFDB	Conventional Forces Data Base
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CJTF	Commander Joint Task Force
COA	Course of Action
COCOM	Combatant Command (Command Authority)
COE	Corps of Engineers
COI	Community of Interest
COP	Common Operational Picture
CS	Cooperative Security
C/S/A	Combatant Commands, Services, and Agencies
CSA	Combat Support Agency
CSV	Comma Separated Value
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DIEA	Defense Information Enterprise Architecture
DIL	Disconnected, Intermittent or Limited bandwidth
DISA	Defense Information Systems Agency
DISAM	Defense Institute of Security Assistance Management

DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoJ	Department of Justice
DoS	Department of State
DOTMLPF and Policy	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy
DRRS	Defense Readiness Reporting System
DSAMS	Defense Security Assistance Management System
DSCA	Defense Security Cooperation Agency
DSCIS	DTRA Security Cooperation Information System
DST	Decision Support Tool
DTRA	Defense Threat Reduction Agency
DTSA	Defense Technology Security Administration
FBI	Federal Bureau of Investigation
FCC	Functional Combatant Command
FEMA	Federal Emergency Management Agency
FMF	Foreign Military Financing
FMS	Foreign Military Sales
FO/GO	Flag Officers/General Officers
GCC	Geographic Combatant Command
GDF	Guidance for Development of the Force
GEF	Guidance for Employment of the Force
GES	Global Information Grid (GIG) Enterprise Services
GIG	Global Information Grid
G-TSCMIS	Global – Theater Security Cooperation Management Information System
HA	Humanitarian Assistance
HHS	Health and Human Services
IA	Information Assurance
IMET	International Military Education and Training
IP	Internet Protocol
IPL	Integrated Priority List
IT	Information Technology
JCCD	Joint Combat Capability Developer
JCRM	Joint Capability Requirements Manager
JCTD	Joint Capability Technology Demonstration
JFC	Joint Force Commander
JOA	Joint Operations Area
JOP	Joint Operation Planning

JOPP	Joint Operation Planning Process
JPME	Joint Professional Military Education
JROC	Joint Requirements Oversight Council
JTIMS	Joint Training Information Management System
KML	Keyhole Markup Language
KPP	Key Performance Parameter
KSA	Key System Attribute
LOO	Line of Operation
MOE	Measure of Effectiveness
MOP	Measure of Performance
MSP	Mission Strategic Plan
NCES	Net-Centric Enterprise Services
NECC	Net-Enabled Command Capability
NGB	National Guard Bureau
NIPRNET	Non-secure Internet Protocol Router Network
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organization
NSS	National Security System
OAA	Operations, Actions, and Activities
OCR	Office of Collateral Responsibility
OHASIS	Overseas Humanitarian Assistance Shared Information System
OPORD	Operation Order
OPR	Office of Primary Responsibility
OPSEC	Operations Security
OSD (P)	Office of the Secretary of Defense (Policy)
OV	Operational View
PII	Personally Identifiable Information
PKO	Peace Keeping Operation
PMO	Program Management Office
POC	Point of Contact
POM	Program Objective Memorandum
QA	Quality Assurance
RFF	Request For Forces
ROE	Rules of Engagement
SA	Situational Awareness
SAN	Security Assistance Network
SAO	Security Assistance Organization
SAT	Security Assistance Team

SC	Security Cooperation
SCETC	Security Cooperation Education & Training Center
SCG	Security Cooperation Guidance
SCIP	Security Cooperation Information Portal
SCORM	Sharable Content Object Reference Model
SFA	Security Force Assistance
SIPRNET	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SMEB	Significant Military Exercise Briefing
SNS	Social Network Service
SOA	Service-Oriented Architecture
SOP	Standard Operating Procedures
SPAWAR	Space and Naval Warfare Systems Command
SPG	Strategic Planning Guidance
SSTR	Stability, Security, Transition and Reconstruction
TCP	Theater Campaign Plan
TEPMIS	Theater Engagement Planning Management Information System
TISC	Transnational Information Sharing Cooperation
TMS	Training Management System
TOPAS	Theater Operational Planning and Assessment Service
TPFDD	Time-Phased Force and Deployment Data
TRADOC	U.S. Army Training and Doctrine Command
TSCMIS	Theater Security Cooperation Management Information System
TSO	Theater Strategic Objective
TTP	Tactics, Techniques, and Procedures
UCP	Unified Command Plan
USAID	United States Agency for International Development
WMD	Weapons of Mass Destruction

(INTENTIONALLY BLANK)

D-8

Appendix E – References

1. Deputy Secretary of Defense Memorandum, Designation of Joint Functional Sponsor and Acquisition Agent for DoD's Global Theater Security Cooperation Management Information System (G-TSCMIS), 10 December 2008
2. Guidance for the Employment of the Force (GEF), 21 April 2008
3. Deputy Secretary of Defense QDR Execution Roadmap, Building Partnership Capacity, 22 May 2006
4. Department of Defense Directive (DoDD) 4630.5 Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) 5 May 2004 (Current as of 23 April 2007)
5. DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation, 24 October 2008
6. DoDD 8320.02, Data Sharing in a Net-Centric Department of Defense, 2 December 2004 (Certified current as of 23 Apr 2007)
7. Department of Defense Instruction (DoDI) 1322.26, Development, Management, and Delivery of Distributed Learning, 16 June 2006
8. Chairman Joint Chiefs of Staff Instruction (CJCSI) 3113.01A, Responsibilities for the Coordination and Review of Security Cooperation Strategies, 18 October 2006
9. CJCSI 3170.01G, Joint Capabilities Integration and Development System, 1 March 2009
10. Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), Online Version, Revised 31 July 2009
11. CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 December 2008
12. Joint Publication 3-08, Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, Volume I, 17 March 2006
13. Joint Publication 5-0, Joint Operation Planning, 26 December 2006
14. Military Contribution to Cooperative Security (CS) Joint Operating Concept, Version 1.0, 19 September 2008
15. Net-Enabled Command Capability (NECC) Capability Development Document (CDD), Version 1, 7 June 2007
16. US Joint Forces Command, Adaptive Planning Concept of Operations, Version 5.0, 1 July 2009 (In final staffing.)
17. Department of Defense Office of the Chief Information Officer, Defense Information Enterprise Architecture, Version 1.0, 11 April 2008
18. DoD Architecture Framework (DoDAF), Version 2.0, 28 May 2009
19. Report of the Defense Science Board Task Force, Department of Defense Policies and Procedures for the Acquisition of Information Technology, March 2009
20. Joint Combat Capability Developer (JCCD) Management Plan Version 1.0, 16 July 2007
21. DoD 5105.38-M, "Security Assistance Management Manual (SAMM)," 3 October 2003

(INTENTIONALLY BLANK)

E-2

Appendix F - Key Performance Parameters and Key System Attributes

The following Key Performance Parameters (KPPs) and Key System Attributes (KSAs) are from the Joint Requirements Oversight Council (JROC)-approved Net-Enabled Command Capability (NECC) Capability Development Document (CDD).

Table 7: NECC CDD KPPs

Key Performance Parameter	Development Threshold	Development Objective
<p>KPP# 1 Shared Situational Awareness: Provide key and vital information via net-centric services on the disposition of friendly, enemy, neutral, and unknown forces to allow the effective exercise of command and control.</p>	<p>Conduct track management and/or be able to access for filter and display, 100,000 or more friendly, enemy, neutral and unknown tracks, at all sites responsible for providing track information to decision makers at all levels of command and control.</p>	<p>Provide users access to unlimited number of tracks and track information to decision makers at all levels of command and control.</p>
<p>KPP# 2 Planning and Execution: Provide warfighters at all levels of command and control contingency and crisis action planning, force deployment / sustainment / redeployment and mission execution capability in support of National Security Objectives and the Adaptive Planning and Execution process.</p> <p>Provide warfighters at all levels of command and control the ability to maintain force readiness and to report on the ability of forces, units, weapons, or equipment to deliver the outputs for which they were designed at the tactical, operational and strategic levels.</p>	<p>Conduct contingency and crisis action planning, force deployment, sustainment, redeployment, and mission execution activities via generation and modification of TPFDD files, query and production of reports, managing and maintaining user accounts and reference with TPFDD validation in support of OPORD / OPLAN for Crisis Action Planning in less than 96 hours and less than 12 hours for Contingency Planning from decision to execution resulting in a success rating of 80 percent and no warfighter incident reports containing significant or critical operational impact.</p> <p>Update readiness database records with maintenance activities to produce and verify accurate reports concerning forces, units, weapons, systems and equipment at the UIC (tactical) and OPLAN (operational) levels with a success rating of 90 percent and no warfighter incident reports containing significant or critical operational impact.</p>	<p>Conduct contingency and crisis action planning, force deployment, sustainment, redeployment, and mission execution activities via generation and modification of TPFDD files, query and production of reports, managing and maintaining user accounts and reference files simultaneously from multiple geographic locations with TPFDD validation in support of OPORD / OPLAN for Crisis Action Planning in less than 24 hours and less than two hours for Contingency Planning from decision to execution.</p> <p>Update readiness database records with maintenance activities via multiple applications to produce and verify accurate reports at multiple locations via multiple applications concerning forces, units, weapons, systems and equipment at the UIC (tactical) and OPLAN (operational) levels with a frequency of readiness database updates available throughout the systems in less than three hours and historical updates less than 24 hours.</p>

Key Performance Parameter	Development Threshold	Development Objective
<p>KPP# 3 System Training: NECC shall provide dynamic, capabilities-based training support tools, either embedded or via the web, across the full range of integrated operations.</p>	<p>Training support tools must be assessed for ease of use and training support effectiveness as favorable by 70 percent of JS/C/S/A users in an operationally representative test environment.</p>	<p>Units must be capable of simultaneously conducting training exercises in Live, Virtual, and Constructive environments using modeling and simulation tools, either embedded or via the web.</p>
<p>KPP# 4 Net Ready: Net-Ready: The system must support Net-Centric military operations. The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.</p>	<p>The system must fully support execution of joint critical operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for transition to Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs, 3) NCOV RM Enterprise Services, 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Approval to Operate (IATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing* specified in the applicable joint and system integrated architecture views.</p> <p>* Data processing is defined as: The input, output, verification, organization, storage, retrieval, transformation and extraction of information from data.</p>	<p>The system must fully support execution of all operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs, 3) NCOV RM Enterprise services, 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Approval to Operate (ATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing* specified in the applicable joint and system integrated architecture views.</p>

Table 8: NECC CDD KSAs

Key System Attribute	Development Threshold	Development Objective
<p>KSA# 1 Situational Awareness: NECC shall provide net-centric services capable of accessing, sharing (send and receive), collating, & displaying COP and CTP information at the source level of accuracy in a format tailored by the user for all physical domains, all components of the joint force, and special operations forces.</p> <p>Essential CTP and COP elements are:</p> <ul style="list-style-type: none"> - Location/status/intentions of friendly forces (current & planned) - Location/identity/status/ intentions of hostile forces (current & projected) - Location/Intentions of other forces/actors (neutral forces, NGOs, etc.) (current & projected) - Meteorological and Oceanographic (Current & forecast environmental conditions and their effects on weapons systems and operations) - Geospatial information - Political/diplomatic information (current & projected) - Media reports - Ensure appropriate access to data based on clearance validation and attributes associated with the data, users, processes or environment - Location status of medical, humanitarian assistance, and terrorist events - Archived / historical COP data 	<p>Integration of land, air/space, maritime/littoral & intelligence information into a Common Tactical Picture in support of the Common Operating Picture (COP).</p> <p>Display and update user requested COP information at the level of accuracy produced within 15 seconds of user request using standard message formats.</p> <p>Provide 3D visualization of, amplification of and reference to source data for friendly, enemy, neutral and unknown tracks, as well as ISR and logistics (deployment and distribution) data, in Near Real-Time (NRT), contained in a database capable of processing 20,000 or more tracks per user defined allocation table.</p> <p>Subjective determination of degree to which a visual representation meets the requirements of 80% of the users, by user (1-5 scale: 1 fully, 5 unmet).</p>	<p>Integration of land, air/space, maritime/littoral & intelligence information into a CTP in support of the COP.</p> <p>Display and update user requested COP information at the level of accuracy produced in 1.0 second or less of user request using standard & non-standard message formats.</p> <p>Provide 3D visualization of, amplification of and reference to source data for friendly, enemy, neutral and unknown tracks, as well as ISR and logistics (deployment and distribution data) in Near Real-Time (NRT), contained in a database capable of processing an unlimited number tracks per user defined allocation table such that the shared situational awareness available to any NECC user regardless of the geographic viewing area, the scale of the geographic viewing area or type track being filtered is not limited by processing and storage capabilities of the system.</p> <p>Subjective determination of degree to which a visual representation meets the requirements of 100% of the users, by user (1-5 scale: 1 fully, 5 unmet)</p>
<p>KSA#2 Planning: (Planning & Execution in support of National Security Objectives)</p> <p>NECC shall provide the capability for distributed collaboration for the development and revision of plans and for plans execution.</p>	<p>Provide vertical and horizontal distributed collaboration for development of force generation, sustainment and projection requirements from CCDR level to JTF/JTF component level.</p>	<p>Provide vertical and horizontal collaboration for development of force generation, sustainment and projection requirements from DoD level down to lowest deployable entity as defined by the Services.</p>

Key System Attribute	Development Threshold	Development Objective
KSA#2 Planning: (continued) Essential elements are: - Distributive and Collaborative Planning Synchronous and asynchronous collaboration services Readiness and Operational Capability Identification (sourcing) - Movement, Sustainment and Tracking - Reduce planning cycle time	System shall be able to allow up to 1,500 simultaneous users per plan and up to 45,000 simultaneous users on the system.	System shall be able to allow up to 3,000 simultaneous users per plan and up to 75,000 simultaneous users on the system.
	System shall provide simultaneous access to all essential elements of collaborative services for all members of all the boards, centers, cells and any other activities within a JTF HQ and between a JTF HQ, CCDR and the JTF Components.	System shall provide near real time collaboration for all members of a JTF, including the edge tactical user, US Agencies, NGOs, Allied and Coalition Partners, DoD COEs, Joint Staff (JS), other Communities of Interest pertinent to the JTF, and between the other JTFs and CCDRs.
	<ul style="list-style-type: none"> • Synchronous collaboration services to include: <ul style="list-style-type: none"> • Persistent workspaces for every board, center, cell and other established activities <ul style="list-style-type: none"> - Concurrent access to 150 sessions • Non-persistent sessions for Ad Hoc meetings <ul style="list-style-type: none"> - Concurrent access to 500 sessions • Session participant metrics: <ul style="list-style-type: none"> - 75% shall have 10, or fewer, participants - 20% shall have 200, or fewer, participants - 5% shall have 1000, or fewer, participants • Scalability <ul style="list-style-type: none"> - Sessions shall have the ability to scale (prioritize) and structure collaborative services in order to accommodate session users within system limitations • Presence and Awareness <ul style="list-style-type: none"> - All Users shall be able to view the current collaboration status of any other authorized user to 98% accuracy • Audio conferencing 	Provide asynchronous messaging services to include: <ul style="list-style-type: none"> • Guaranteed delivery person-to-person and organizational messaging in support of record traffic environments • A strong mechanism for message origin authentication, non-repudiation, and guaranteed delivery. • Survivability alerts

Key System Attribute	Development Threshold	Development Objective
KSA#2 Planning: (continued)	<ul style="list-style-type: none"> • Chat/ instant messaging • Shared file space • Video teleconferencing • Shared whiteboard • Asynchronous collaboration services for 4000 users to include: <ul style="list-style-type: none"> • Person-to-person and organizational messaging (e.g., E-mail) • Delivery of alerts <ul style="list-style-type: none"> – Within 30 seconds • Web Portal 	
	<p><u>Crisis Action Planning and Execution</u> (after release of warning order)</p> <ul style="list-style-type: none"> - Support development and maintenance cycles for OPORD and associated products: < 96 hours - Time required to perform a readiness assessment: < 6 hours 	<p><u>Crisis Action Planning and Execution</u> (after release of warning order)</p> <ul style="list-style-type: none"> - Support development and maintenance cycles for OPORD and associated products: < 24 hours - Time required to perform a readiness assessment: < 2 hours
	<p><u>Contingency Planning</u> (upon receipt of a planning directive)</p> <ul style="list-style-type: none"> - Support development and maintenance cycle for OPLAN and associated products: < 12 months - Time required to perform a readiness assessment: < 48 hours 	<p><u>Contingency Planning</u> (upon receipt of a planning directive)</p> <ul style="list-style-type: none"> - Support development and maintenance cycle for OPLAN and associated products: < 2 months - Time required to perform a readiness assessment: < 24 hours
	<p><u>Total Force Visibility</u> Changes to current readiness data/information are visible globally within 2 hours of input.</p> <ul style="list-style-type: none"> - Track inventory readiness, availability, and apportionment down to the individual level, and respond to queries within 10 minutes of initial request. - Provide automatic notification of dual tasking within 5 minutes of force sourcing. 	<p><u>Total Force Visibility</u> Changes to current readiness data/information are visible globally NRT of input.</p> <ul style="list-style-type: none"> - Provide continuous check for potential dual tasking during force sourcing process and provide immediate notification when and if it occurs. <p>Continuous and uninterrupted Track to asset level visibility</p> <ul style="list-style-type: none"> - Provide continuous and uninterrupted Track to asset level visibility; globally track inventory, readiness, availability and apportionment of all forces

Key System Attribute	Development Threshold	Development Objective
<p>KSA#2 Planning: (continued)</p>	<p><u>Track to asset level visibility</u></p> <ul style="list-style-type: none"> - User queries across disparate data sources will identify the authoritative data source. <p>Reports or Queries will be delivered in less than 7 seconds from the time query is issued at 99.999% accuracy.</p>	<p>down to the individual level, and respond to queries within 1 minute of initial request.</p> <p><u>Track to asset level visibility</u></p> <ul style="list-style-type: none"> - User queries across disparate data sources will identify the authoritative data source. <p>Reports or Queries will be delivered in less than 2 seconds from the time query is issued at 99.999% accuracy.</p>
<p>KSA#3 Training Support: NECC shall provide, either embedded or via the web, training support tools to facilitate effective individual and collective team, staff and unit training.</p> <p>Essential training elements to enable individual, collective and conceptual training:</p> <ul style="list-style-type: none"> - Designed in "ease of use" to minimize the need for extensive use of mobile training teams and resident schools to achieve individual and collective proficiency with NECC tools -Alert/notification of new training provided with new spiral capability - Web-based Training - Web-based transfer -Capability to support distributed exercises -Embedded Modeling and Simulation capability - Learning Management System for training managers 	<p>Ease of use and training support effectiveness must be assessed as meeting current IT industry benchmarks for ease of use, the current Joint National Training Capability (JNTC) construct and supporting JT FC attributes and metrics.</p> <ul style="list-style-type: none"> - Help tools, diagnostic proficiency assessment tools, and training management tools must be embedded or available via the web to facilitate assessment and tracking of individual and collective proficiency. - Training tools must be available via the web - Training and remedial, on-demand support must be web transferable - Must have alerts to notify training managers of training updates and new capability. <p>Individual:</p> <ul style="list-style-type: none"> - 70% of functional users (JS/C/S/A) judge NECC training capability as favorable in a standard Operational Test environment - 70% of Systems Administrators judge NECC training capability as favorable in a standard Operational Test environment 	<p>Conceptual:</p> <ul style="list-style-type: none"> - Meets all T2 standards of and is fully integrated with JKDDC and JNTC.

Key System Attribute	Development Threshold	Development Objective
KSA#3 Training Support: <i>(continued)</i>	Collective: - Individuals and or units must be able to conduct training on operational systems without affecting real world picture/data. Conceptual: - Supports the learning and training attributes of Training Transformation (T2) as defined by Joint Knowledge Development and Distribution Capability (JKDDC), JNTC and Joint Assessment and Enabling Capability (JAEC). - Supports JT FC attributes and metrics.	
KSA #4: Technical Refresh: Technical refresh enables the program to leverage information technology advances to provide enhanced warfighter capabilities within scope and budget of the NECC program.	1. Inherent performance and technical upgrades gained through hardware modernization. (e.g., improved processors, etc.)	N/A
	2. Level-of-effort software development to maintain system interfaces with upgraded networks and with other interdependent systems (e.g., new standards for Information Assurance, etc.)	
	3. Refined Key Supporting Attributes requirements, (e.g., Improved Integration of land, air/space, maritime/littoral and intelligence information into a Common Operating Picture (COP) etc.)	

(INTENTIONALLY BLANK)

F-8