

MARINE CORPS SYSTEMS COMMAND



C4I INTEROPERABILITY AND INTEGRATION MANAGEMENT PLAN (C4I I&IMP)

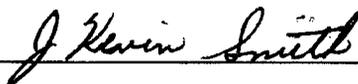
2 September 2005

THIS PAGE INTENTIONALLY LEFT BLANK

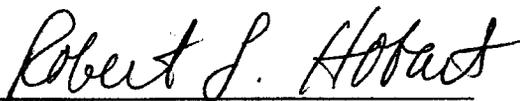
**Marine Corps Systems Command
Command, Control, Communications, Computers, and Intelligence
Interoperability and Integration Management Plan
(MARCORSYSCOM C4I I&IMP)**

IIMP-05-Ver 2

2 September 2005



Mr. J. Kevin Smith
Director, C4I SE&I Division
C4I Integration
Marine Corps Systems Command



Mr. Robert L. Hobart
Deputy Commander, C4I Integration
Marine Corps Systems Command

THIS PAGE INTENTIONALLY LEFT BLANK

**MARCORSYSCOM
C4I INTEROPERABILITY AND INTEGRATION
MASTER PLAN
(C4I I&IMP)**

EXECUTIVE SUMMARY

This document is one in a series of plans being developed to implement command-level oversight of interoperability among the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems under the cognizance of the Commanding General, Marine Corps Systems Command (MARCORSYSCOM). This document describe the procedures, processes, responsibilities and authorities of the various organizations within Marine Corps Systems Command (MARCORSYSCOM) with respect to the cooperative design, development, testing, and fielding of Information Technology (IT) and National Security Systems (NSS), and the manner in which the Deputy Commander, C4I Integration (DC C4I/I), shall manage interoperability and integration.

This C4I I&IMP provides a plan to manage the acquisition of systems to handle the C4I information needs of Marine Corps warfighters, while presenting the lowest feasible logistics burden in the battlespace. It defines the organizational relationships among the various MARCORSYSCOM agencies engaged in acquisition of C4I systems, describes the methods for collaboration on Enterprise C4I I&I information exchange and collaborative decision-making on Enterprise C4I I&I issues, and defines the details of the interrelationships between separate acquisition programs and enterprise-level oversight.

Multiple interoperability and integration topics need to be addressed in order to properly manage interoperability and integration practices to reflect the MARCORSYSCOM product group construct. These are to be addressed, resolved, and published in additional plans. These additional plans are the C4I EIP Configuration Management Plan (C4I ECMP) and C4I EIP Master Test Plan (C4I EMTP), and the planned C4I Enterprise Integrated Product Master Acquisition Strategy (C4I EMAS). Examples of topics that are or shall be addressed in these additional plans are:

- The manner in which MARCORSYSCOM shall perform enterprise-level configuration control. Currently in the C4I ECMP.
- Development and acceptance of a single future-vision architecture that will drive the future development of existing programs; and development and control of the Marine Corps enterprise architecture at the levels of detail necessary to support detailed planning, development, testing, and evaluation. Expected in the planned issue of the C4I EMAS.
- The manner in which the testing and fielding of related products shall be managed and coordinated across the Command. Currently in the C4I EMTP.
- The MARCORSYSCOM plan for and interrelationship of umbrella programs such as JBMC2, FIOP, FORCEnet, etc. Expected in the planned issue of the C4I EMAS.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

DOCUMENT CHANGE HISTORY	1
1 INTRODUCTION	1
1.1 PURPOSE	1
1.2 SCOPE	1
1.3 GOALS	1
1.4 STRUCTURE	1
1.5 CANCELLATIONS	1
2 ORGANIZATIONAL RELATIONSHIPS	3
2.1 OVERVIEW	3
2.2 DEPUTY COMMANDER C4I INTEGRATION (DC C4I/I)	3
2.2.1 Duties	3
2.2.2 Staff Supervision	4
2.2.3 C4I/I Support Group	4
2.3 PRODUCT GROUP DIRECTORS (PGD) AND UNASSIGNED PROGRAM MANAGEMENT OFFICES	5
2.3.1 PGDs	5
2.3.2 Unassigned Program Managers (PM)	5
2.3.3 Responsibilities	5
2.4 EXTERNAL PROGRAM MANAGEMENT OFFICES SUPPORTED BY MARCORSYSCOM	5
2.5 MILESTONE DECISION AUTHORITY	5
3 ENTERPRISE INTEGRATED PRODUCT	7
3.1 PURPOSE	7
3.2 DEFINITION	7
3.3 ENTERPRISE INTEGRATED PRODUCT (EIP) FUNCTIONAL AREAS	7
3.3.1 Warfighting Functional Areas (6)	7
3.3.2 Business Management Areas (8)	7
3.3.3 Communications and Networking	8
3.3.4 The C2 Functional Area	8
4 COLLABORATION AND DECISION-MAKING FOR INTEROPERABILITY AND INTEGRATION FOR THE ENTERPRISE INTEGRATED PRODUCT	9
4.1 REQUIREMENT	9
4.2 DECISION-MAKING STRUCTURE	9
4.3 C4I/I BOARD	10
4.3.1 Enterprise Configuration Control Board	10
4.3.2 EIP Target Board (Target Board)	11
4.4 ENTERPRISE INTEROPERABILITY WORKING GROUP (EIWG)	11
4.5 STANDING WORKING GROUPS	11
4.6 TARGET BOARD WORKING GROUPS	11
5 PROGRAM COORDINATING INSTRUCTIONS	13
5.1 OVERVIEW	13

5.2	INTEGRATED ARCHITECTURE DATABASE.....	13
5.3	CENTRALIZED PLANNING.....	13
5.3.1	<i>EIP Specifications.....</i>	<i>13</i>
5.3.2	<i>Information Support Plans (ISP).....</i>	<i>14</i>
5.3.3	<i>Net-Ready Key Performance Parameters (NR-KPP).....</i>	<i>15</i>
5.4	DE-CENTRALIZED EXECUTION.....	15
5.5	FEDERATION-OF-SYSTEMS PERFORMANCE MEASUREMENT.....	16
5.6	CONFIGURATION BASELINE CAPTURE.....	16
5.6.1	<i>Configuration Status Accounting Report (CSAR).....</i>	<i>17</i>
6	ROLES AND RESPONSIBILITIES.....	19
6.1	DEPUTY COMMANDER C4I INTEGRATION.....	19
6.1.1	<i>C4I Systems Engineering and Integration Division.....</i>	<i>19</i>
6.1.2	<i>Information Assurance and Joint Requirements Division.....</i>	<i>20</i>
6.1.3	<i>Commanding Officer MCTSSA.....</i>	<i>20</i>
6.2	PRODUCT GROUP DIRECTORS.....	20
6.2.1	<i>Program Managers (PMs).....</i>	<i>20</i>
6.2.2	<i>PGDs/PMs.....</i>	<i>20</i>
6.2.3	<i>Project Team Leaders.....</i>	<i>21</i>
6.3	UNASSIGNED PROGRAM MANAGERS.....	21
6.3.1	<i>Project Team Leaders under Unassigned PMs.....</i>	<i>21</i>
	APPENDIX A: ACRONYMS AND TERMINOLOGY.....	A-1
	APPENDIX B: REFERENCES.....	B-1
	APPENDIX C: LIST OF EIP PROGRAMS.....	C-1
	APPENDIX D: C4I INTEGRATION BOARD AND SE&I DIVISION CHARTERS.....	D-1
	APPENDIX E: EIP TARGET BOARD CHARTER & PROCESS.....	E-1
E.1	BACKGROUND.....	E-1
E.2	EIP TARGET BOARD CHARTER.....	E-1
E.3	EIP TARGET BOARD PROCESS.....	E-3
E.4	TARGET BOARD INTEGRATED PRODUCT TEAMS.....	E-6
E.5	TARGET ORIGINATOR’S REQUEST:.....	E-7
	APPENDIX F: ENTERPRISE INTEROPERABILITY WORKING GROUP CHARTER	
F-1	
F.1	PURPOSE.....	F-1
F.2	RELATIONSHIPS.....	F-1
F.3	BACKGROUND.....	F-1
F.4	OBJECTIVE.....	F-2
F.5	MEMBERSHIP.....	F-2
F.6	TASKS.....	F-3
F.7	RESPONSIBILITIES.....	F-4
F.8	ADMINISTRATIVE.....	F-5
F.9	AUTHORITY.....	F-5
F.10	APPROVAL/ENDORSEMENT.....	F-5

ATTACHMENT F-1: HARDWARE WORKING GROUP CHARTER.....	F-1-1
ATTACHMENT F-2: SOFTWARE WORKING GROUP CHARTER	F-2-1
ATTACHMENT F-3: COMMUNICATIONS AND NETWORK WORKING GROUP CHARTER.....	F-3-1
ATTACHMENT F-4: CRYPTOGRAPHIC MODERNIZATION INITIATIVE WORKING GROUP CHARTER	F-4-1
APPENDIX G: ISP DEVELOPMENT PROCESS	G-1
G.1 PURPOSE.....	G-1
G.2 BACKGROUND	G-1
G.3 ISP POLICY.....	G-1
G.3.1 When Required.....	G-1
G.3.2 ISP Timeframe	G-1
G.3.3 ISP Maintenance.....	G-1
G.4 PROCEDURES.....	G-2
G.4.1 Step 1. IA&JR Reviews Program for ISP Requirement.....	G-2
G.4.2 Step 2. Does a CDD or CPD (or draft) exist containing an NR-KPP?.....	G-4
G.4.3 Step 3. No, CDD/CPD (or draft) containing NR-KPP does not exist – PM performs NR-KPP Development Process (ISP).....	G-4
G.4.4 Step 4. Yes, CDD/CPD containing NR-KPP (or draft) does exist. -- PM Completes Draft ISP.....	G-4
G.4.5 Step 5. Initial Review Conducted by IA&JR and C4I SE&I Divisions.....	G-4
G.4.6 Step 6. Final Review Conducted by C4I SE&I, MCTSSA, IA, ACENG, USMC CIO, DON CIO, RDA CHENG and other PMs, as appropriate.....	G-4
G.4.7 Step 7. PGD Signs ISP.....	G-5
G.4.8 Step 8. PM Presents Draft ISP to DC C4I/I.....	G-5
G.4.9 Step 9. Plan Accepted?	G-5
G.4.10 Step 10. IA&JR Submits ISP to OASD for Joint review	G-5
G.4.11 Step 11. Comments from the Joint review forwarded to PM for resolution	G-5
G.4.12 Step 12. PM revises ISP as required and presents it to DC C4I/I.....	G-5
G.4.13 Step 13. Plan Approved?.....	G-6
G.4.14 Step 14. Appropriate Updates Performed.....	G-6
G.4.15 Step 15. Load ISP to JCPAT-E.....	G-6
G.5 THE PROCESS FOR HANDLING 2681s.....	G-6
G.5.1 Step 1. PM Completes draft 2681	G-6
G.5.2 Step 2. Initial Review Conducted by IA&JR and C4I SE&I Divisions.....	G-7
G.5.3 Step 3. Final Review Conducted by C4I SE&I, MCTSSA, IA, ACENG, and other PMs, as appropriate.....	G-7
G.5.4 Step 4. PGD Signs 2681.....	G-7
G.5.5 Step 5. IA&JR sends Draft 2681 to DC C4I/I.....	G-7
G.5.6 Step 6. 2681 accepted?	G-7
G.5.7 Step 7. Appropriate Updates performed.....	G-7
G.6 RESPONSIBILITIES	G-7
ATTACHMENT G-1: ISP ESTABLISHMENT REVIEW PROCESS	G-1-1
TAB 1 to ATTACHMENT G-1: ISP Establishment Review Template	G-1-2
ATTACHMENT G-2: PROCEDURES FOR THE USE OF NON-MARINE CORPS ISPs	G-2-1

APPENDIX H: NR-KPP DEVELOPMENT PROCESS.....	H-1
H.1 PURPOSE.....	H-1
H.2 BACKGROUND.....	H-1
H.3 NR-KPP POLICY.....	H-1
<i>H.3.3.1 When Required.....</i>	<i>H-1</i>
<i>H.3.3.2 NR-KPP Timeframe.....</i>	<i>H-1</i>
<i>H.3.3.3 NR-KPP Maintenance.....</i>	<i>H-1</i>
H.4 PROCEDURES.....	H-1
<i>H.4.3.1 Step A. PM requests NR-KPP from IA&JR (unique to NR-KPP (ISP)).....</i>	<i>H-4</i>
<i>H.4.3.2 Step B. IA&JR requests views from C2 Integration Div (unique to NR-KPP (ISP)).....</i>	<i>H-4</i>
<i>H.4.3.3 Step 1. C4I/I Operations Team receives MCCDC OVs and CRD Crosswalk and sends to IA&JR & C4I SE&I for Action.....</i>	<i>H-4</i>
<i>H.4.3.4 Step 2a. IA&JR Develops Initial TVs.....</i>	<i>H-4</i>
<i>H.4.3.5 Step 2b. IA&JR and C4I SE&I review OVs and CRD Crosswalk, conduct meeting with PM, and provide OVs and initial TVs.....</i>	<i>H-4</i>
<i>H.4.3.6 Step 3. IA&JR sends request to PM for action on SV development.....</i>	<i>H-4</i>
<i>H.4.3.7 Step 4. PM Develops SVs and Compliance Statements.....</i>	<i>H-4</i>
<i>H.4.3.8 Step 5. When SV-6 available, PM gives to IA&JR to start finalizing TVs.....</i>	<i>H-4</i>
<i>H.4.3.9 Step 6. PM sends SVs and Compliance Statements to IA&JR.....</i>	<i>H-4</i>
<i>H.4.3.10 Step 7. C4I SE&I validates SVs and IA&JR finalizes TVs.....</i>	<i>H-5</i>
<i>H.4.3.11 Step 8. IA&JR verifies interfaces to systems listed.....</i>	<i>H-5</i>
<i>H.4.3.12 Step 9A. IA&JR delivers SVs, TVs, and Compliance Statements to MCCDC and copies C4I/I Operations Team for closing action (unique to NR-KPP (JCIDS)).....</i>	<i>H-5</i>
<i>H.4.3.13 Step 9B. IA&JR delivers validated Architecture Views to PM (unique to NR-KPP (ISP)).....</i>	<i>H-5</i>
H.5 DEVELOPING COMPONENTS.....	H-5
H.6 RESPONSIBILITIES.....	H-6
ATTACHMENT H-1: COMPLIANCE STATEMENTS AND ASSOCIATED EFFORTS.....	H-1-1
APPENDIX I: CERTIFICATION AND ACCREDITATION PROCESS.....	I-1
I.1 PURPOSE.....	I-1
I.2 BACKGROUND.....	I-1
I.3 C&A PROCESS.....	I-1
I.4 CHECKLISTS.....	I-2
CERTIFICATION REQUIREMENTS REVIEW.....	I-1-1
CERTIFICATION & ACCREDITATION CHECK-OFF SHEET.....	I-2-1
SSAA PREPARATION CHECKLIST.....	I-3-1
APPENDIX J: SYSTEMS ENGINEERING AND INTEGRATION ASSESSMENTS PROCESS.....	J-1
APPENDIX K: COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, COMBAT AND INTELLIGENCE SYSTEMS MODERNIZATION PROCESS (C5I MP).....	K-1

APPENDIX L: PROCESSES FOR SUPPORT TO GROUPS EXTERNAL TO MARINE CORPS SYSTEMS COMMAND L-1

APPENDIX M: URGENT UNIVERSAL NEED STATEMENT (UNS) PROCESS FOR INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS M-1

LIST OF FIGURES

Figure 2-1: MARCORSYSCOM Organization 3
Figure 3-1: Relationship of Functional Areas to Decision-Maker 8
Figure 4-1: C4I I&I Decision Making Structure 10
Figure 5-1: De-Centralized Staff Supervision by DC C4I/I 16
Figure E-1: The EIP Target Board Process E-4
Figure E-2: Feedback to Originator for EIP Target Process E-5
Figure E-3: Development Process for Marine Corps Positions on Joint/Naval/Coalition Issues....
..... E-6
Figure E-1-4: EIP Target Board Process E-1-1
Figure F-1: EIWG Organizational Relationship F-1
Figure G-1: ISP Preparation and Approval Process G-3
Figure G-2: 2681 Preparation and Approval Process G-6
Figure H-4-1: NR-KPP Development Process (JCIDS) H-4-2
Figure H-4-2: NR-KPP Development Process (ISP) H-4-3
Figure H-4-3: DoDAF Architecture Product Flow H-4-6
Figure I-1: Certification and Accreditation (C&A) Process I-3
Figure M-1: Urgent UNS Process for C4ISR M-1

LIST OF TABLES

Table G-1: ISP Submission Timetable and Required Joint Reviews. G-2
Table M-1: Urgent UNS-Required Sections of SSAA M-2
Table M-2: Urgent UNS-Required Architecture Products M-3
Table M-3: Points of Contact M-4

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION.

1.1 Purpose

The purpose of the Command, Control, Communications, Computers, and Intelligence (C4I) Interoperability and Integration Management Plan (C4I I&IMP) is to describe the procedures, processes, responsibilities and authorities of the various organizations within Marine Corps Systems Command (MARCORSYSCOM) with respect to the cooperative design, development, testing, and fielding of Information Technology (IT) and National Security Systems (NSS).

1.2 Scope

This document is intended to govern the interoperability and integration (I&I) of all IT and NSS as identified in the Department of Defense (DoD) Directive 4630.5 reference (a) under the acquisition management of MARCORSYSCOM. It specifically includes systems fielded to both the operating forces and the supporting establishment under the research, development, acquisition, fielding, and lifecycle management of MARCORSYSCOM. It also provides guidance for systems under the acquisition oversight of other agencies that are supported from MARCORSYSCOM.

1.3 Goals

The strategic goal of the C4I I&IMP is to field a war-winning C4I information handling system which meets the current and emerging needs of Marine Corps warfighters while presenting the lowest feasible logistics burden in the battlespace. Objectives to achieving this goal are:

- Define the organizational relationships among the various MARCORSYSCOM agencies engaged in acquisition of C4I systems (Section 2).
- Describe and identify the Enterprise Integrated Product (EIP) and associated functional areas (Section 3).
- Describe the methods for collaboration on Enterprise C4I I&I information exchange and collaborative decision-making on Enterprise C4I I&I issues (Section 4).
- Define the details of the interrelationships between separate acquisition programs and enterprise-level oversight (Section 5).
- Identify the roles and responsibilities of the various MARCORSYSCOM agencies engaged in acquisition of C4I systems (Section 6).

1.4 Structure

The objectives of this C4I I&IMP, described in sections 2-6, are supported by detailed appendices. Appendices A, B, and C provide the acronyms and terminology, references, and the list of EIP programs. Appendix D is the C4I Integration Board and C4I SE&I Team charters, Appendix E is the EIP Target Board charter and process, and Appendix F is the Enterprise Interoperability Working Group (EIWG) and subgroup charters. Appendices G, H and I describe the Information Support Plans (ISP) and Net-Ready KPP (NR-KPP) development and certification and accreditation (C&A) processes. Appendices J, K, and M describe SE&I assessments, Command, Control, Communications, Computers, Combat and Intelligence Modernization Process (C5I MP), and Urgent Universal Need Statement (UNS) processes.

1.5 Cancellations.

This document replaces the following publications, orders, and policy statements:

- Marine Corps Systems Command, “C4I Interoperability and Integration Management Plan (C4I I&IMP)”, 19 April 2004

THIS PAGE INTENTIONALLY LEFT BLANK

2 ORGANIZATIONAL RELATIONSHIPS.

2.1 Overview.

The organization of MARCORSYSCOM is depicted in figure 2-1. Command relationships are usually shown in circular form in order to emphasize the collaboration and teamwork that is the hallmark of the Command. See reference (b) for further details.

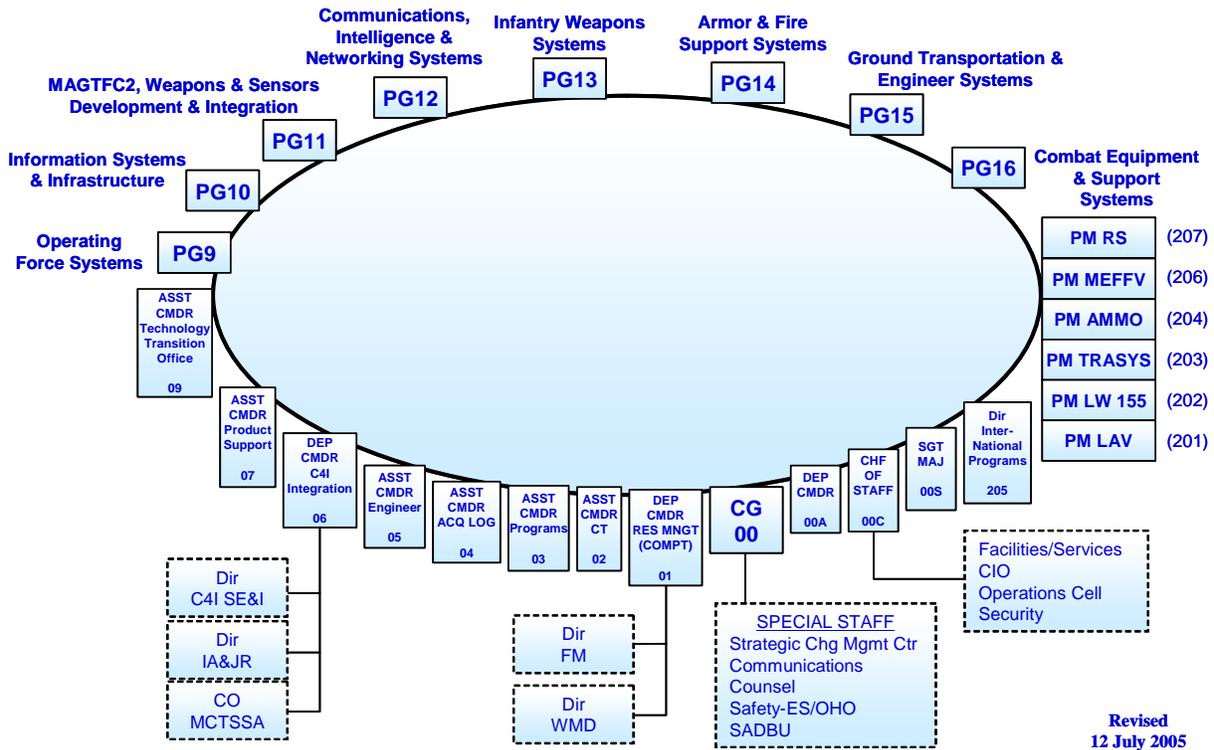


Figure 2-1: MARCORSYSCOM Organization

2.2 Deputy Commander C4I Integration (DC C4I/I).

2.2.1 Duties.

Assigned duties of the DC C4I/I are:

- Bring together the appropriate product group directors and unassigned program managers (PM) for integration decision-making;
- Lead the C4I/I Support Group, which includes but is not limited to planning, test and analysis of the EIP;
- Support the transformation of the Marine Corps Tactical Systems Support Activity (MCTSSA) into a Systems Integration Environment;
- Manage the C4I/I Support Group to accomplish configuration management of the EIP, to provide analytical support to the C4I/I Support Group, and to execute EIP tasking;
- Represent the Command and the Commanding General on external C4I I&I working groups;
- Apply interoperability and integration policies and procedures in this document to outside agencies that acquire NSS and IT systems for the entire United States Marine Corps (USMC) IT Enterprise;

- Serve as the Designated Approval Authority (DAA) for all systems and applications developed by MARCORSYSCOM, and other Marine Corps entities when requested;
- Act as the System and Technical View Architect for the Marine Corps Enterprise Architecture, and lead the resolution of any conflicts with the Operational View Architecture.

2.2.2 Staff Supervision.

The DC C4I/I develops C4I I&I policy and exercises staff supervision over C4I I&I execution. Staff supervision is defined as:

“The process of advising other staff officers and individuals subordinate to the commander of the commander’s plans and policies, interpreting those plans and policies, assisting such subordinates in carrying them out, determining the extent to which they are being followed, and advising the commander thereof.” (Joint Publication 1-02 “DoD Dictionary of Military and Associated Terms” (reference (c))).

2.2.3 C4I/I Support Group.

The DC C4I/I leads the C4I/I Support Group (SG06) within the Command. SG06 consists of the C4I Systems Engineering and Integration (C4I SE&I) Division (SG061), the Information Assurance and Joint Requirement (IA&JR) Division (SG062) and the Marine Corps Tactical Systems Support Activity (MCTSSA) (SG063). Additional teams under the C4I/I Support Group are the Technology Transfer Team and the Operations Team.

- C4I SE&I Division. The C4I SE&I Division supports command-level oversight for the Commanding General MARCORSYSCOM of C4ISR system engineering and integration, and leads the team of C4ISR system engineering professionals in the instantiation and maintenance of the Marine Corps Enterprise IT Architecture. See Appendix D for the C4I SE&I Charter.
- Information Assurance and Joint Requirements Division. The Information Assurance (IA) and Joint Requirements (IA&JR) Division supports the C4I/I systems engineering process by leading an IA program for MARCORSYSCOM which includes the certification and accreditation of all tactical and strategic C4ISR Automated Information Systems (AIS), C4ISR Information Security support, and Program Objective Memorandum (POM) support of Communications Security hardware and software to the Marine Corps. Additionally, the IA&JR Division provides USMC representation to joint standards working groups, supports program managers in preparing ISPs, oversees the implementation of Joint standards within programs, as well as managing the integrity and configuration of the Marine Corps Architecture Support Environment (MCASE) repository.
- MCTSSA. MCTSSA supports the C4I/I systems engineering process by establishing a Systems Integration Environment (SIE) to support analysis of C4ISR systems interoperability and integration. MCTSSA also supports joint interoperability certification by the Joint Interoperability Test Command (JITC) for acquisition programs. Additionally, MCTSSA operates as a Joint Distributed Engineering Plant (JDEP) participant, and provides assistance to the operating forces to remedy interoperability and integration problems encountered with fielded C4ISR systems. Lastly, MCTSSA provides direct software engineering support to acquisition product teams when requested.
- Technology Transfer Team. The Technology Transfer Team supports the C4I/I systems engineering process through the identification and integration of evolving technologies that

provide improved capability to existing and planned USMC C4ISR systems, and provides input to the various Military Capability Package (MCP) initiatives and Future Naval Capabilities (FNC) initiatives regarding the technical maturity and risk of transition to an acquisition program.

- Operations Team. The Operations Team supports the C4I/I systems engineering process through its business model, inclusive of administrative and personnel management, coordination of command taskers, and other activities related to the efficiency of the C4I/I Infrastructure. Additionally, the Operations Team supports staff activity coordination.

2.3 Product Group Directors (PGD) and Unassigned Program Management Offices.

2.3.1 PGDs.

PGDs are responsible to the Commanding General, MARCORSYSCOM for the execution of their assigned acquisition programs according to existing regulations and policies. Each PGD maintains a Strategic Business Team (SBT), which includes a group-level systems engineer.

2.3.2 Unassigned Program Managers (PM).

Unassigned PMs perform the same functions as the PGDs, usually for a smaller number of programs. Some unassigned PMs maintain a systems engineering capability on the program manager's support staff, in lieu of a full strategic business team (SBT).

2.3.3 Responsibilities.

The PGDs and unassigned PMs within MARCORSYSCOM participate in policy development and the resolution of C4I I&I issues through their collaboration on the C4I/I Board. Systems engineers within the SBTs and the unassigned PM offices support the execution of C4I I&I policies through their interactions with the product team leaders and system engineers; they also assist in identifying and resolving I&I issues through their active participation in the EIWG. System engineers assigned to product teams carry out the C4I I&I policies within their assigned teams and assist in identifying and resolving I&I issues through their active participation in the standing working groups of the EIWG and the Target Board Working Groups.

2.4 External Program Management Offices Supported by MARCORSYSCOM.

There are several program management offices outside of MARCORSYSCOM that are supported to various degrees by MARCORSYSCOM agencies. The largest of these is the Direct Report Program Manager for Advanced Amphibious Assault (DRPM AAA). Usually, these offices work in a collaborative way with the DC C4I/I. Though C4I I&I policies developed within MARCORSYSCOM are not necessarily mandatory for their programs, they are often mandatory for many of the systems that are integrated into their system.

2.5 Milestone Decision Authority.

Milestone Decision Authority (MDA) is derived from the DoD 5000 series documents, references (d) and (e). Nothing in this C4I I&IMP is intended to supersede the Milestone Decision Authority. However, the C4I SE&I Division will submit an independent evaluation of a system's performance against its interoperability and integration goals as a part of the milestone decision process in support of programs for which the CG is the MDA, and when requested by other MDAs.

THIS PAGE INTENTIONALLY LEFT BLANK

3 ENTERPRISE INTEGRATED PRODUCT

3.1 Purpose.

The EIP is the name given to the collection of all of the systems or components that are under the staff supervision of the DC C4I/I. It is a theoretical management construct, only. It incorporates warfighting systems, business management systems, and the IT and communications portions of weapons systems. It does not require changes to the current MDA's or PGDs' supervision of programs; nor does it require changes to the current methods for controlling resources within the Command.

3.2 Definition.

The EIP is defined as all systems under the direct cognizance of the Commanding General MARCORSYSCOM or drawing resource support from MARCORSYSCOM which:

- Meet the Clinger-Cohen criteria; that is systems which connect in any way with DOD data networks, either tactical or non-tactical;
- Connect to other C4ISR networks, such as Joint Tactical Information Distribution System (JTIDS), Link 16, voice circuits and networks, and the Integrated Broadcast Service (IBS);
- Have future potential to connect to the networks above;
- Include the C4ISR component of platforms where the systems above are installed during normal operations;
- Provide support to the systems above that use digital communications, such as training systems, special and general-purpose test equipment.

In addition, some systems are included in the EIP for monitoring purposes, even if they are under acquisition authority in other system commands, as long as they are routinely used by the Marine Corps.

3.3 Enterprise Integrated Product (EIP) Functional Areas.

The programs and systems within EIP are divided into sixteen functional areas for analysis. Figure 3.1 depicts the relationship of these functional areas to the decision-maker.

3.3.1 Warfighting Functional Areas (6).

These include:

- Systems for the control of maneuver and direct fires,
- Systems for the control of intelligence,
- Systems for the control of indirect fires,
- Systems for the control of logistics,
- Systems for the control of force protection,
- Systems for the control of air operations.

3.3.2 Business Management Areas (8).

These include:

- Systems used to support or manage the development of doctrine,

Supporting the Decision-Maker

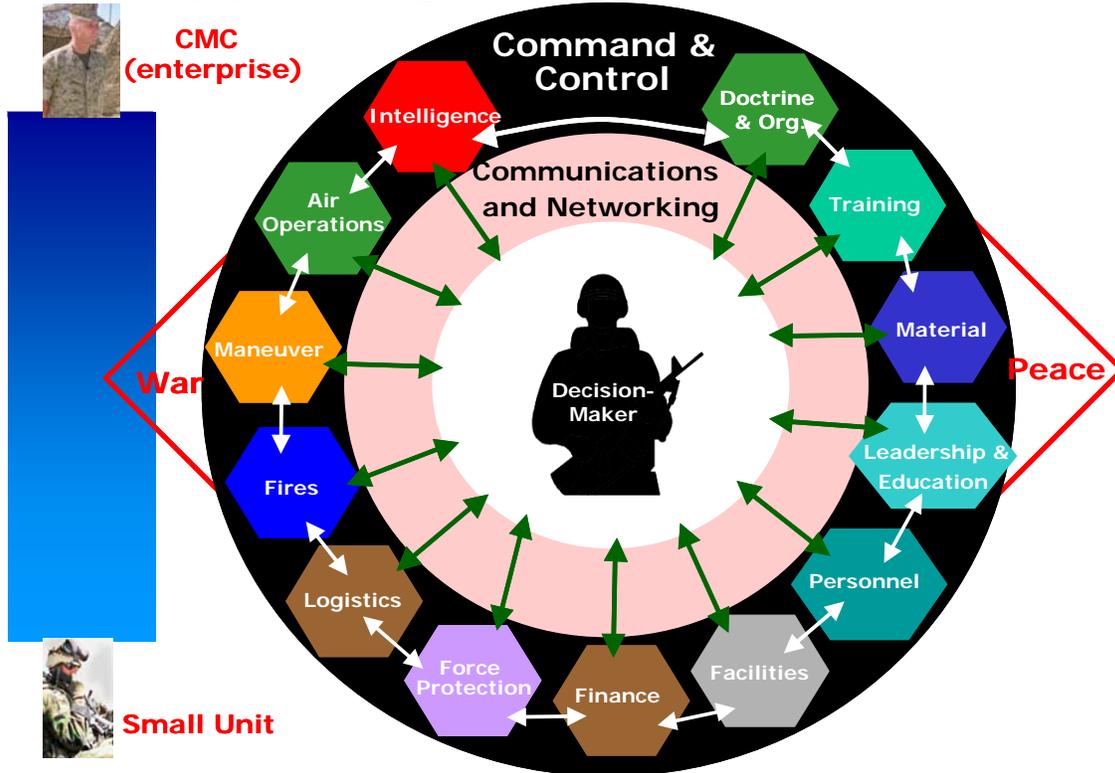


Figure 3-1: Relationship of Functional Areas to Decision-Maker

- Systems used to administer, support or manage the development of Marine Corps organizations,
- Systems used to support or manage training,
- Systems used to support or manage material development, including acquisition, research and development, and scientific exploration,
- Systems used to support or manage leadership and education,
- Systems used to support or manage personnel administration,
- Systems used to support, operate, or manage Marine Corps facilities,
- Systems used to conduct financial operations.

3.3.3 Communications and Networking.

Systems used for communications and networking, either tactical or administrative, and common IT components form a single functional area.

3.3.4 The C2 Functional Area.

The C2 functional area includes systems that provide oversight into the other functional areas taken as a group, systems that support commanders' direct decision-making, and systems that support dissemination of the decision-maker's orders but are not included in any other functional area.

4 COLLABORATION AND DECISION-MAKING FOR INTEROPERABILITY AND INTEGRATION FOR THE ENTERPRISE INTEGRATED PRODUCT

4.1 Requirement.

Control of C4I I&I within MARCORSYSCOM is a staff supervision function; it is necessary to collaborate within the Command on issues affecting C4I I&I. The need exists to respond to C4I I&I issues emerging from internal factors, such as cross-product-group planning and execution, C4I I&I policy development, and EIP configuration control. Also, the need exists to collaborate within the Command on responses to external factors such as:

- Joint Battle Management C2 (JBMC2)
- Global Information Grid (GIG)
- Common Operating Environment (COE) and GIG Enterprise Services (GES)
- Army Future Combat System (FCS)
- Navy Seapower 21 and FORCEnet
- Air Force Constellation Architecture
- Joint Family of Integrated Operational Pictures
- Issues from the Marine Corps Operating Forces
- Issues with interoperability between systems developed by MARCORSYSCOM and those developed by other systems commands.

In addition to collaboration within the Command, other affected Marine Corps stakeholder organizations must be consulted when making decisions or policies that affect MARCORSYSCOM products. Some of these include: Headquarters Marine Corps (HQMC), Marine Corps Combat Development Command (MCCDC), Marine Corps operating forces and the reserve component, Marine Corps base commands, Marine Corps Enterprise Network operators, and the systems commands of the other Services. The USMC CIO roles and responsibilities MOA, reference (s), defines the interaction between HQMC, MCCDC and MCSC with respect to IT systems, including NSS.

4.2 Decision-Making Structure.

The decision-making structure for this C4I I&IMP is depicted in figure 4-1. It consists as a three-tiered decision tree, including the C4I Integration Board, the EIWG, and standing and temporary working groups. Issues are assigned to standing and temporary working groups with detailed subject-matter knowledge in order to develop recommended decisions; these decisions are reviewed at the EIWG by senior systems engineers within the Command and representatives of the appropriate stakeholder organizations; the recommendations are then forwarded to the C4I Integration management board for final approval. The Target Board process is described in Appendix E.

C4I I&I Governance Strategy Collaboration and Decision-Making

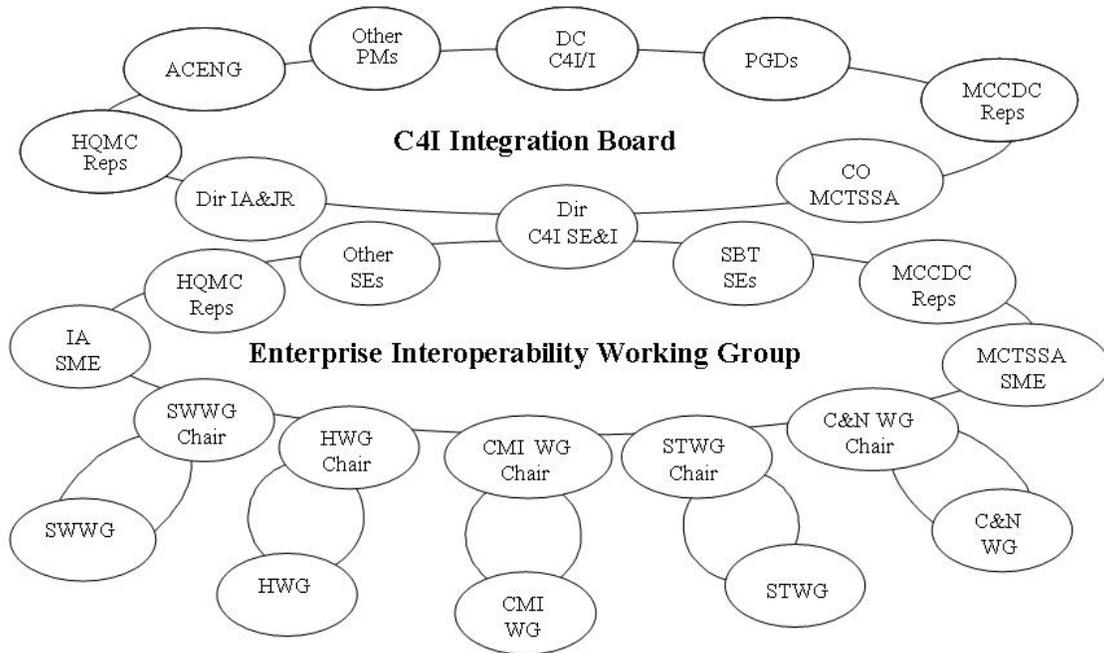


Figure 4-1: C4I I&I Decision Making Structure

4.3 C4I/I Board.

The C4I/I Board meets monthly. This board is led by the DC C4I/I. Membership consists of:

- Deputy Commander, C4I Integration
- Assistant Commander, Engineering
- Directors of all MARCORSSYSCOM product groups,
- Commanding Officer MCTSSA,
- Program Managers of MARCORSSYSCOM programs not assigned to a product group,
- Division heads of the C4I/I Support Group,
- Representatives from HQMC (C4),
- Representatives from MCCCDC (C2I).

The C4I/I Board is a formal meeting and is open to agenda items from all members. Its purpose is to provide a forum for coordination of efforts and issues across product groups and to coordinate current and future C4I I&I plans. The charter for the C4I/I Board is provided at Appendix D. Depending on the issues to be addressed, the C4I Integration Board may also function as the Enterprise Configuration Control Board (ECCB) or the Target Board.

4.3.1 Enterprise Configuration Control Board.

The ECCB is formed from the members of the C4I/I Board. Refer to the ECMP for a list of ECCB members. The ECCB is the principal organization for enterprise-level configuration management of the EIP. Procedures for configuration management of the EIP are contained in

the EIP Configuration Management Plan (ECMP), reference (f). The ECCB will be convened quarterly, or when required.

4.3.2 EIP Target Board (Target Board).

The Target Board is formed from the members of the C4I/I Board. Refer to Appendix E for a list of Target Board members. The Target Board's purpose is to advise the DC C4I/I on the impacts of technical and non-technical issues that affect the interoperability of MARCORSSYSCOM C4I systems that are beyond the scope of any individual PGD to resolve and that may require significant coordination or investigative effort to resolve. The Target Board may be asked to address interface configuration management issues when a consensus cannot be achieved at lower levels. The Target Board will be issue-oriented and normally meets quarterly in March, June, September, and December. Target Board meetings will be held on the same day as the C4I/I Board meeting for the selected months and either precede or follow that meeting. The Target Process is described in Appendix E to this C4I I&IMP.

4.4 Enterprise Interoperability Working Group (EIWG).

The EIWG provides the working-level coordination necessary to prepare and submit C4I I&I recommendations to the C4I Integration Board for decisions. This working group, led by the C4I SE&I Division, consists of the lead system engineers from each product group, subject-matter leaders from MCTSSA, engineering representatives from each unassigned program manager and appropriate engineering representatives from MCCDC and HQMC. The EIWG makes recommendations to the C4I/I Board regarding proposed changes to enterprise configuration items, C4ISR data elements and Marine Corps positions on Joint/Combined interoperability standards. The EIWG is responsible for conducting configuration management of the Marine Corps C4ISR architecture and Joint/Combined interoperability standards. The EIWG is also responsible for providing routine oversight and coordination of the standing working groups as well as any Target Board working groups that might be formed. The charter for the EIWG is contained in Appendix F.

4.5 Standing Working Groups.

The C4I/I Board has approved five Standing Working Groups. They include the Hardware Working Group (HWG), Software Working Group (SWWG), Communications and Network Working Group (C&N WG), the Cryptographic Modernization Initiative Working Group (CMI WG) and the Standards Working Group (STWG). The purpose of these teams is to develop recommendations on courses of action for resolving interoperability and integration issues within their designated specialty areas. The charters for the Standing Working Groups are contained as Attachments to the EIWG charter in Appendix F. These Standing Working Groups are intended to operate for a long term. If their intended operation, under the governance of the EIWG, changes or no longer exists, the EIWG may recommend that the C4I/I Board disband them or redirect their focus.

4.6 Target Board Working Groups.

Target Board Working Groups may be chartered as defined in Appendix E. When so chartered, they will operate under the governance of the EIWG until their assignment is completed, at which time the C4I/I Board will disband them.

THIS PAGE INTENTIONALLY LEFT BLANK

5 PROGRAM COORDINATING INSTRUCTIONS

5.1 Overview.

The DC C4I/I exercises staff supervision of interoperability and integration of NSS and IT systems within MARCORSYSCOM. These responsibilities are described in Sections 1 and 2. See DOD Dictionary of Military and Associated Terms, Joint Publication 1-02 (reference (c)) or Appendix A for a definition of staff supervision.

The DC C4I/I leads the C4I/I Support Group (SG06) within the Command. SG06 consists of C4I SE&I Division (SG061), IA&JR Division (SG062), MCTSSA (SG063), Technology Transfer Team and Operations Team. The method chosen to exercise staff supervision involves centralized planning, de-centralized execution, periodic performance measurement of the EIP federation-of-systems (FedOS¹), and the capture of the tested FedOS configuration. This supervision method is consistent with practices in the operating forces for mission-type command and control. See Marine Corps Doctrinal Publication 6 (MCDP-6), Command and Control (reference (v)), for a discussion of the differences between detailed command and control and mission command and control.

Each of the activities, used for the oversight of interoperability and integration of NSS and IT systems within MARCORSYSCOM, is described in the paragraphs below.

5.2 Integrated Architecture Database.

The key support tool for effective staff supervision of C4I I&I is the existence of an authoritative C4I integrated architecture database. This integrated architecture database is the Marine Corps Architecture Support Environment (MCASE). MCASE provides the source data for preparing all architectural views produced by MARCORSYSCOM. The database contains detailed, specific information on command node functions, required operational interfaces and information exchange requirements, and C4ISR systems used to support information exchange requirements. Access to this database is available to all agencies involved in concept development, requirements definition, system design and acquisition, test agencies, training facilities, field activities, and agencies engaged in other life-cycle support of Marine Corps systems.

5.3 Centralized Planning.

The DC C4I/I does not have line authority for programs within the EIP federation of systems; rather, the DC C4I/I exercises staff supervision for the interoperability and integration of these systems.

5.3.1 EIP Specifications.

There are no specifications to describe the EIP. Each system within the FedOS maintains its own set of system-level specifications. The DC C4I/I defines the EIP by means of the Marine Corps Integrated Architecture Picture (MCIAP). This is a stylized High-Level Operational Concept Graphic (OV-1), combined with a depiction of the assignment of systems to enterprise nodes, System Interface Description, Nodal Perspective (SV-1). It combines in one depiction an Operational View 1 (OV-1) and System View 1 (SV-1) for Marine Corps organizations. This depiction provides decision-making support and a high-level view to assist PMs and Product Teams to understand the interface requirements for their systems. The MCIAP is developed from the combined integrated architecture database (MCASE).

¹ See Appendix A for the definition.

5.3.2 Information Support Plans (ISP)

Changes to the Joint Capabilities Integration and Development System (JCIDS) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 (reference (g)), DoD Instruction (DODI) 4630.8 (reference (h)), and CJCSI 6212.01 (reference (i)) replace the C4ISP with the ISP and further require an ISP for every IT and NSS. The DC C4I/I uses the ISP, and it's associated Net-Ready KPP (NR-KPP), as a tool to specify detailed interface requirements to program managers and to manage the execution of interface development. The DC C4I/I is the approval authority for all ISPs at all Acquisition Category (ACAT) levels, Abbreviated Acquisition Programs (AAPs), Non-ACAT, and for fielded programs for all MARCORSSYSCOM-managed programs.

The DC C4I/I assigns C4I I&I goals to each system or program by requiring their development and production be traceable to the Marine Corps Enterprise Architecture. This is done through the DC C4I/I's approval of the system or program's architectural views contained in the systems' ISP or associated documents. The system views (SVs) contained in the CDDs and CPDs, also know as JCIDS documents, and the SVs in ISPs are developed by the Project Office in coordination with IA&JR, incorporated into the integrated architectural database, and provide the next level of detail down from the MCIAP. They are tailored to the operational requirements of the individual system.

The technical views (TVs) provided in these documents are developed by IA&JR in coordination with the project office. IA&JR develops the initial draft of the TVs, submits them to the PM, who coordinates changes with IA&JR. IA&JR incorporates changes and submits the final TVs for inclusion in appropriate documents. The TVs will specify not only system specification requirements, but also policies internal to the EIP that are necessary to ensure that the system under development conforms to the EIP Master Acquisition Strategy (to be issued), in addition to policies and procedures mandated by external Agencies. The ISP also describes the product team leader's plans for including the requirements described in the operational, system, and technical views for the product in the development and testing of the system.

The ISP is approved by the DC C4I/I following endorsements by the PM of the system under development, (including concurrence of the PMs of the systems which support and/or have interfaces to the system under development), the associated PGD, and the Director IA&JR, and after appropriate staffing to the Joint Staff. Once approved, the ISP becomes a configuration control item under the EIP, to be managed within the scope of the ECMP (reference (f)). Changes to a system's ISP require approval by the DC C4I/I. Appendix G of this plan contains procedures for preparation, approval, and modification of the ISP.

ISPs and associated NR-KPPs are required for every ACAT program, non-ACAT program, AAP, and fielded systems undergoing upgrades for all IT and NSS. In the event that an ISP is not required for an EIP system, the program shall be required to submit a minimum set of architectural views for approval by the DC C4I/I. These minimum set of views are currently the SV-2, SV-6, SV-8 and TV-1 (also known as a 2681), but others may be required. Examples where an ISP may not be required and a 2681 is required is for an already fielded system not being upgraded and not needing JITC certification or an ATO. Another example would be for a system used but not developed by the Marine Corps, and the developing Service does not have an appropriate ISP showing Marine Corps interfaces. Once the 2681 is approved, this minimum set stands in lieu of the ISP for the program until its next system upgrade and creation of a full ISP including an NR-KPP.

Specific procedures for developing and processing ISPs are contained in Appendix G. Additional guidance is available from the ISP Team of the IA&JR Division. A web-enabled repository for ISPs (MCASE) has been established in order to facilitate and monitor changes to these documents.

5.3.3 Net-Ready Key Performance Parameters (NR-KPP)

The focus of the new joint interoperability and supportability process is the NR-KPP. The NR-KPP assesses net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability. The NR-KPP will be developed earlier in the acquisition process as part of the JCIDS documentation; however systems that do not have an approved JCIDS document will be required to develop an NR-KPP as part of developing their ISP. The NR-KPP consists of four components: Information Assurance; compliance with the Net-Centric Operations and Warfare Reference Model (NCOW-RM); compliance with applicable GIG Key Interface Profiles (KIPs); and supporting integrated architecture products. NR-KPPs are found in the Capabilities Development Document (CDD), Capability Production Document (CPD), and when there is no CDD or CPD, in the system's ISP (e.g. for ORD-based requirements).

ISPs and their associated NR-KPPs are now the key management link between the DC C4I/I and the product team, used within the Command to facilitate interoperability and integration among the IT systems within all product groups and programs. The NR-KPP includes the DoD Architecture Framework products associated with each IT system, and will be included or referenced in each ISP. Specific procedures for developing and processing NR-KPPs are contained Appendix H.

5.4 De-Centralized Execution.

Because constituent systems of the EIP FedOS are developed and managed independently within the various product groups and program management offices, the DC C4I/I uses a method of de-centralized staff supervision during the execution portion of the C4I I&IMP. The process by which this is accomplished differs, depending on who is the MDA, as depicted in figure 5-1. For those programs where the PGD is the MDA, the EIP Systems Engineer will compare the Functional Configuration Audit (FCA) and/or the Product Configuration Audit (PCA) with the architecture products provided in the NR-KPP. This will be done in conjunction with the Strategic Business Team System Engineer review of the program as part of the review of the ISP required at each milestone review and major system upgrade. For all other programs, the EIP System Engineer will follow the process described in Appendix J in order to fulfill his responsibilities in the Milestone Assessment Team (MAT). During this phase of the plan, the EIP System Engineer works with the respective SBT Lead Engineer and Project Engineer during the Milestone Team Assessment (MTA) process, to confirm that the goals set in the ISP are being met. For example, complete FCA and PCA reports will meet this requirement. In the event that no FCA or PCA has been completed, more detailed analysis will be required using other programmatic documents

In addition to monitoring program execution as described above, the EIP System Engineer is responsible for facilitating the resolution of emerging issues between the programs within the EIP or among MARCORSYSCOM programs and those of external agencies; particularly when: issues cannot be resolved at lower echelons, the issues cross PGD boundaries, or they require command-level action.

During this phase, the C4I SE&I Division will, upon request and in coordination with the appropriate PGD or independent PM, assign C4I system engineers to product teams in Product Groups Infantry Weapons Systems (PG-13), Armor and Fire Support Systems (PG-14), Ground Transportation and Engineer Systems (PG-15), and Combat Equipment and Support Systems (PG-16), as well as to unassigned program management offices.

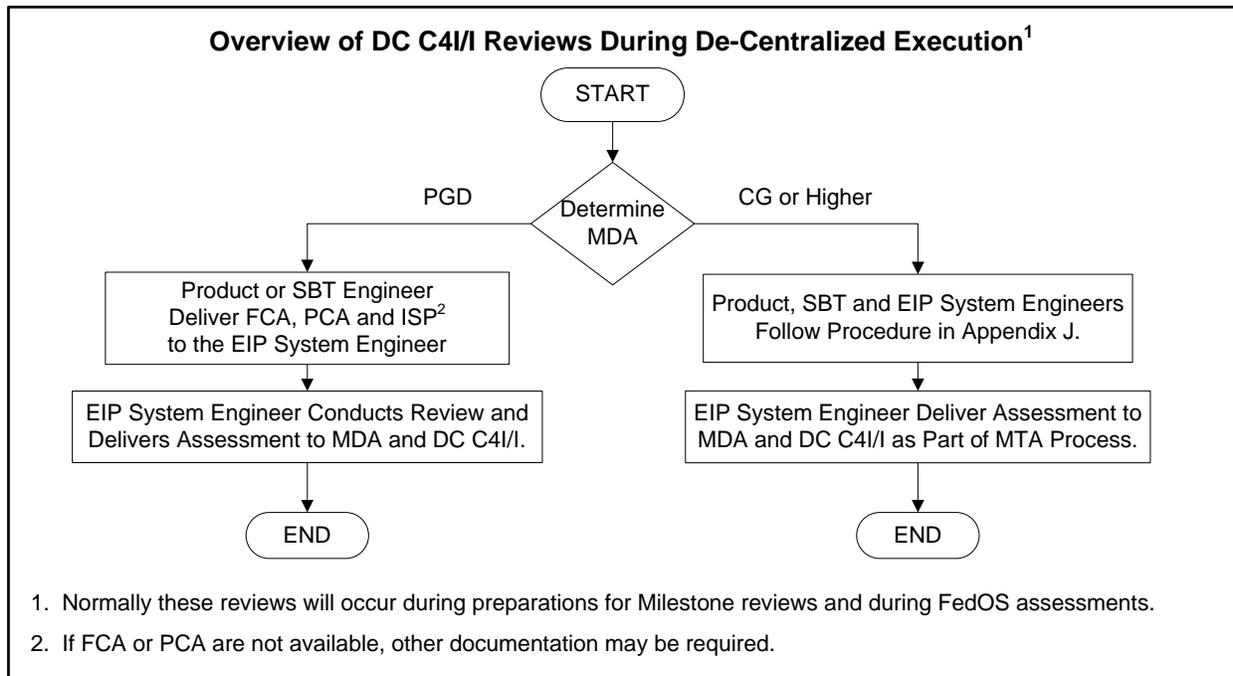


Figure 5-1: De-Centralized Staff Supervision by DC C4I/I

5.5 Federation-of-Systems Performance Measurement.

The DC C4I/I needs a quantitative way to measure the performance of interoperability and integration for the EIP FedOS. To achieve this, the EIP Test Director shall conduct an assessment of the impact of fielding new systems within the EIP on an annual basis. The results of this testing will be documented in a report to the DC C4I/I and to the Commanding General; copies will be provided to the PGDs and unassigned PMs. The detailed processes and procedures for conducting EIP assessments and analyses are described in the EIP Master Test Plan, reference (j).

Normally, EIP programs will first be selected for FedOS assessments in the year in which they achieve acquisition Milestone C. They will be expected to participate in FEDOS testing during every year in which they continue to be under active development. Programs may be relieved of their requirement for annual FEDOS participation at the discretion of the DC C4I/I when they are no longer under development or undergoing upgrades. Otherwise, they are eligible for FEDOS assessments every year until they are removed from service in the operating forces or supporting establishment.

5.6 Configuration Baseline Capture.

The EIP System Engineer shall record the configurations of the systems that participate in the annual FedOS test as well as the configurations of those systems that were eligible to participate but did not do so. This will become the EIP Product Baseline for that fiscal year FedOS test.

5.6.1 Configuration Status Accounting Report (CSAR).

The EIP baseline is documented in an EIP CSAR. The CSAR is published quarterly and provides an executive-level summary of the EIP configuration.

THIS PAGE INTENTIONALLY LEFT BLANK

6 ROLES AND RESPONSIBILITIES.

The paragraphs below describe the roles and responsibilities for those involved in the management and success of the EIP.

6.1 Deputy Commander C4I Integration.

The Deputy Commander C4I Integration (DC C4I/I) is responsible for:

- Collaborating to make value-added integration decisions, and chairing the C4I/I Board, ECCB, and Target Board meetings.
- Managing the configuration of the Enterprise Architecture and producing an accurate Configuration Status Accounting Report quarterly.
- Assisting in the achievement of successful Milestone Decisions/Post Production Block Upgrades with respect to I&I. This includes coordinating the development of Information Support Plans (ISP) for MARCORSYSCOM systems across all appropriate architecture and development organizations, and providing final approval for the ISPs; also acting as the approval authority for ISPs of MARCORSYSCOM programs, any subsequent changes to approved ISPs, and any requests for waivers or delays.
- Serving as the Designated Approval Authority (DAA) for all systems and applications developed by MARCORSYSCOM, reference (u).
- Ensuring proactive conformance to interoperability standards, including establishing the process for development of Marine Corps positions on Joint interoperability standards, providing tailored interoperability specifications, and establishing the EIP.

6.1.1 C4I Systems Engineering and Integration Division.

The C4I SE&I Division supports command-level oversight for MARCORSYSCOM of C4ISR system engineering and integration within the Command and leads the team of C4ISR system engineering professionals in the instantiation and maintenance of the Marine Corps Enterprise Architecture. This is accomplished by:

- Providing support to the DC C4I/I in the area of C4ISR systems engineering and integration for the Marine Corps C4I Enterprise, to include I&I, commonality, architecture, new technology insertion, and overall strategy for the Enterprise.
- Establishing and executing processes necessary to manage interoperability of C4ISR systems across MARCORSYSCOM using a command-wide strategy of centralized planning and decentralized execution. Developing and maintaining the Marine Corps C4ISR Systems and Technical Architecture, and Enterprise information in a series of MCIAP integrated views.
- Establishing and executing the processes necessary to ensure that MARCORSYSCOM C4ISR systems interoperate with the appropriate systems of the other Services and joint commanders.
- Providing programmatic representation for Marine Corps technical requirements to external program offices and other agencies when the product is not otherwise assigned to a MARCORSYSCOM product group, independent PM or DRPM. Providing the engineering, interoperability and integration support for Marine Corps C4ISR systems integration aboard naval platforms, and act as the Marine Corps representative to the Navy Command, Control, Communications, Computers, Combat and Intelligence Modernization Process (C5I MP).

- Establishing and executing processes for providing direct support to MARCORSYSCOM and MARCORSYSCOM-supported product teams.
- Supporting the DC C4I/I in ensuring proactive conformance to interoperability standards, confirming that the goals set in the ISP are being met in conjunction with the MTA.

6.1.2 Information Assurance and Joint Requirements Division.

The IA&JR Division supports the systems engineering process by providing an information assurance program for MARCORSYSCOM to include the certification and accreditation (C&A) for all tactical and strategic C4ISR AISs, C4ISR Information Security support, and Program Objective Memorandum (POM) support of Communications Security (COMSEC) hardware and software to the Marine Corps. This is accomplished by:

- Providing support to the DC C4I/I in the area of C4ISR systems information assurance, to include the C&A process, and support to joint requirements.
- Serving as the IA Certification Authority for all systems and applications developed by MARCORSYSCOM.
- Assisting PMs to prepare ISPs for DC C4I/I approval.
- Submitting approved and revised ISPs to higher headquarters.
- Maintaining the MCASE repository and a library of all approved ISPs and other C4I system engineering documentation.

6.1.3 Commanding Officer MCTSSA.

The Commanding Officer (CO) MCTSSA is responsible for:

- Providing technical support to the Commanding General, MARCORSYSCOM, and Program Managers to acquire and sustain C4ISR products for the Operating Forces.
- Providing technical support to the operating forces conducting force protection, anti-terrorism and counter terrorism operations using fielded command and control systems, and providing remedies for I&I problems encountered with fielded C4ISR systems.
- Providing technical support to the DC C4I/I for C4ISR systems engineering and integration, establishing a Systems Integration Environment (SIE), and providing sufficient resources to support EIP verification and certification.
- Providing support as a Joint Distributed Engineering Plant (JDEP) participant.

6.2 Product Group Directors.

PGDs are responsible for oversight of systems engineering for systems within their product groups and for resolving interoperability issues between systems within their product groups. PGDs are responsible for the identification of irresolvable interoperability and integration issues between systems in different product groups.

6.2.1 Program Managers (PMs).

PMs are responsible for oversight of engineering management for systems under their cognizance, and for resolving interoperability issues between systems within their programs.

6.2.2 PGDs/PMs.

The PGDs and PMs are collectively responsible for:

- Ensuring compliance with this C4I I&IMP.

- Participating with IA&JR Division in screening the Command Automated Program/Information System (CAPS) to determine a need for ISPs and maintaining the program data in the CAPS database and system/technical data in MCASE.

6.2.3 Project Team Leaders.

Project Team Leaders are responsible for:

- Inserting, modifying, deleting, and yearly auditing their system's data in MCASE.
- Adhering to this C4I I&IMP.

6.3 Unassigned Program Managers

Unassigned PMs are responsible for:

- Providing oversight of engineering management for systems under their cognizance.
- Resolving interoperability issues between systems within their programs.
- Identifying irresolvable interoperability and integration issues between systems in different product groups or Unassigned PMs.
- Ensuring compliance with this C4I I&IMP.
- Participating with IA&JR Division in screening the Command Automated Program/Information System (CAPS) to determine a need for ISPs and maintaining the program data in the CAPS database and system/technical data in MCASE.

6.3.1 Project Team Leaders under Unassigned PMs.

Project Team Leaders under Unassigned PMs are responsible for:

- Inserting, modifying, deleting, and yearly auditing their system's data in MCASE.
- Adhering to this C4I I&IMP.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: ACRONYMS AND TERMINOLOGY

ACRONYMS

2681: SV-2, SV-6, SV-8 and TV-1

AAO: Authorized Acquisition Objective

AAP: Abbreviated Acquisition Program

AAVS: Amphibious Assault Vehicle Systems

ABL: Allocated Baseline

ACAT: Acquisition Category

ACENG: Assistant Commander, Engineering

ADWS: Air Defense Weapons Systems

AIS: Automated Information System

APM: Assistant Program Manager

ASD/C3I: Assistant Secretary of Defense, Command, Control, Communications and Intelligence

ASP: Application Security Plan

ATO: Authority to Operate

ATC: Authority to Connect

BMADS: Battlespace Management and Air Defense Systems

BPA: Blanket Purchasing Agreement

BCT: BMADS Coordination Team

C&A: Certification and Accreditation

C&N: Communications and Networks

C2: Command and Control

C4: Command, Control, Communication, and Computers

C4I I&IMP: C4I Interoperability and Integration Management Plan

C4I: Command, Control, Communication, Computers and Intelligence

C4ISP: C4I Support Plan

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

C5I MP: Command, Control, Communications, Computers, Combat and Intelligence Modernization Process

CA: Certification Authority

CAPS: Command Automated Program/Information System
CCA: Clinger-Cohen Act
CCR: Communications Certification Request
CDA: Central Design Activity/Agent
CDD: Capabilities Design Document
CDR: Critical Design Review
CG: Commanding General
CGS: Common Ground Station
CIO: Chief Information Officer
CISC: Complex Instruction Set Computer
CJCSI: Chairman Joint Command Staff Instruction
CJCSM: Chairman Joint Command Staff Manual
CMF: Common Message Format
CMI: Cryptographic Modernization Initiative
CMP: Configuration Management Plan
CNO: Chief of Naval Operations
CNRWG: Combat Net Radio Working Group
CNSS: Committee on National Security Systems
CO: Commanding Officer
COA: Course of Action
COE: Common Operating Environment
COMSEC: Communications Security
COTS: Commercial Off-the Shelf
CPD: Capabilities Production Document
CRD: Capstone Requirements Document
CRR: Certification Requirements Review
CSAR: Configuration Status Accounting Report
CSFL: Common System Function List
CSIS: Combat Support Information Systems
DAA: Designated Approving Authority
DASN: Deputy Assistant Secretary of the Navy
DC C4I/I: Deputy Commander, C4I Integration
DC/A: Deputy Commandant for Aviation

DCMS: Director of COMSEC Material System

DHS: Department of Homeland Security

DIR C4I SE&I: Director, C4I Systems Engineering and Integration Division

DIR IA&JR: Director, Information Assurance and Joint Requirements

DIRNSA: Director, National Security Agency

DISA: Defense Information Systems Agency

DISR: DoD Information Technology Standards Registry

DITSCAP: Department of Defense (DoD) Information Technology Security Certification and Accreditation Process

DMI: Data Management and Interoperability

DoD: Department of Defense

DoN: Department of the Navy

DOTMLPF: Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities

DR: Design Review

DRPM AAA: Direct Report Program Manager, Advanced Amphibious Assault

DRPM: Direct Report Program Manager

DT: Developmental Test

ECCB: Enterprise Integrated Product (EIP) Configuration Control Board

ECMP: Enterprise Integrated Product (EIP) Configuration Management Plan

EECP: EIP Engineering Change Proposal

EIP: Enterprise Integrated Product

EITA: Enterprise IT Architecture

EIWG: Enterprise Interoperability Working Group

EKMS: Electronic Key Management System

EPL: Evaluated Product List

EW: Electronic Warfare

eXNET: Expeditionary Network

FAR: Federal Acquisition Regulations

FBL: Functional Baseline

FCA: Functional Configuration Audit

FCS: Future Combat Systems

FedOS: Federation of Systems

FIT: Functional Integration Team

FNC: Future Naval Capabilities
FRP: Full Rate Production
FRP: Fleet Response Plan
FY: Fiscal Year
GCSS-MC: Global Combat Support System-Marine Corps
GENSER: General Service
GES: GIG Enterprise Services
GIG: Global Information Grid
HQMC: Headquarters Marine Corps
HQMC C4: Headquarters Marine Corps, C4/CIO
HWG: Hardware Working Group
I&I: Interoperability and Integration
IA: Information Assurance
IA&JR: Information Assurance and Joint Requirements
IAS: Intelligence Analysis System
IATC: Interim Authority to Connect
IATO: Interim Approval to Operate
IAVA: Information Assurance Vulnerability Alert
IAW: In Accordance With
IBS: Integrated Broadcast Service
ICD: Initial Capabilities Document
ICP: Interface Change Proposal
ICTO: Interim Certificate to Operate
IDD: Interface Design Description
IDIQ: Indefinite Delivery Indefinite Quantity
IEEE: Institute of Electrical and Electronics Engineers
IER: Information Exchange Requirement
IOB: Interoperability Branch
IPD: Integrated Product Development
IPR: In-Progress Review
IPT: Integrated Product Team
IRM: Information Resources Management
IRS: Interface Requirements Specification

ISNS: Integrated Shipboard Network System
ISO: International Organization for Standardization
ISP: Information Support Plan
IT: Information Technology
IT-21: Information Technology for the 21st Century
ITI: Information Technology Infrastructure
ITP: Interoperability Test Panel
ITS: Information Technology System
J/N/C: Joint/Naval/Coalition
JBMC2: Joint Battle Management Command and Control
JCIDS: Joint Capabilities Integration and Development System
JCPAT-E: Joint C4I Program Assessment Tool - Empowered
JDEP: Joint Distributed Engineering Plant
JFCOM: Joint Forces Command
JIC: JITC Interoperability Certification
JINTACCS: Joint Interoperability of Tactical Command and Control Systems
JITC: Joint Interoperability Test Command
JKMIWG: Joint Key Management Infrastructure Working Group
JMSWG: Joint Multi-Tactical Data Link Standards Working Group
JMTCCB: Joint Multi-Tactical Data Link Configuration Control Board
JSCMWG: Joint Service Cryptographic Modernization Working Group
JSTARS: Joint Surveillance Target Attack Radar System
JT2 IPT: Joint Transformation to Tactical Data Enterprise Services (TDES) Integrated Product Team
JTA: Joint Technical Architecture
JTADG: Joint Technical Architecture Development Group
JTIDS: Joint Tactical Information Distribution System
JTRS: Joint Tactical Radio System
KIP: Key Interface Profile
KMI: Key Management Infrastructure
KPP: Key Performance Parameter
LAN: Local Area Network
LCCE: Life Cycle Cost Estimate

LRIP: Low Rate Initial Production
MAGTF: Marine Air-Ground Task Force
MAIS: Major Automated Information System
MARCORSYSCOM: Marine Corps Systems Command
MARFOREUR: Marine Forces Europe
MARFORLANT: Marine Forces Atlantic
MARFORPAC: Marine Forces Pacific
MARFORRES: Marine Forces Reserves
MAT: Milestone Assessment Team
MATCOM: Material Command
MC: Mission Critical
MCAP: Marine Corps Application Portfolio
MCASE: Marine Corps Architecture Support Environment
MCCDC: Marine Corps Combat Development Command
MCDP: Marine Corps Doctrinal Publication
MCEB: Military Communications-Electronics Board
MCEN: Marine Corps Enterprise Network
MCHS: Marine Common Hardware Suite
MCIAP: Marine Corps Integrated Architecture Picture
MCMO: Marine Corps Communications Security Management Office
MCNOSC: Marine Corps Network Operations and Security Command
MCO: Marine Corps Order
MCOTEA: Marine Corps Operational Test and Evaluation Activity
MCP: Military Capabilities Package
NCR: Navy Change Request
MCTCA: Marine Corps Transformational Communications Architecture
MCTSSA: Marine Corps Tactical Systems Support Activity
MCWL: Marine Corps Warfighting Laboratory
MDA: Milestone Decision Authority
MDAPS: Major Defense Acquisition Programs
ME: Mission Essential
MEB: Marine Expeditionary Brigade
MEF: Marine Expeditionary Force

MIP: MAGTF C4ISR Integrated Package
MNS: Mission Needs Statement
MS: Milestone
MSARC: Marine Systems Acquisition Review Council
MTA: Milestone Team Assessment
MTS: Marine Tactical System
NAVAIRSYSCOM: Naval Air Systems Command
NAVCOMPT: Navy Comptroller
NBC: Nuclear, Biological, and Chemical
NCES COE: Network-Centric Enterprise Services Common Operating Environment
NIPRnet: Non-Secure Internet Protocol Router Network.
NMCI: Navy-Marine Corps Intranet
NSA: National Security Agency
NSS: National Security System
NUWG: Network Users Working Group
OASD: Office of the Assistant Secretary of Defense
OASD (NII): OASD (Network Information and Infrastructure)
OC: Operations Center
ONI: Office of Naval Intelligence
ORD: Operational Requirement Document
OSD: Office of the Secretary of Defense
OT&E: Operational Test and Evaluation
OT: Operational Test
OV: Operational View
PBBE: Performance-Based Business Environment
PBL: Product Baseline
PCA: Product Configuration Audit
PDA: Program Decision Authority
PDR: Preliminary Design Review
PEO: Program Executive Office
PG: Product Group
PGD: Product Group Director
PKE: Public Key Enabled

PKI: Public Key Infrastructure
PM: Program Manager
PMM: Program Manager Marine
PMO: Program Management Office
PO: Project Officer
POA&M: Plan of Action and Milestones
POC: Point of Contact
POM: Program Objective Memorandum
POR: Program of Record or Program Office of Record
PQDR: Program Quadrennial Review
PTL: Project Team Leader
RDA: Research, Development and Acquisition
RS: Radar Systems
RISC: Reduced Instruction Set Computer
SBT: Strategic Business Team
SE&I: Systems Engineering and Integration
SE&ISD: Systems Engineering and Integration Support Division
SEMP: Systems Engineering Management Plan
SG: Support Group
SIE: Systems Integration Environment
SIPRnet: Secret Internet Protocol Router Network
SME: Subject Matter Expert
SOS: System of Systems
SPAWAR: Space and Warfare Systems Command
SPD: Solution Planning Directive
SRR: System Requirements Review
SSAA: System Security Authorization Agreement
STWG: Standards Working Group
SV: System View
SWWG: Software Working Group
SYSCOM: Systems Command
T&E: Test and Evaluation
TACC: Tactical Air Command Center

TACSIIP: Tactical Systems Interoperability and Integration Program

TAOC: Tactical Air Operations Center

TCAC: Technical Control Analysis Center

TDDS: TRAP Data Dissemination System

TDIMF-G: Tactical Data Intercomputer Message Format – G

TDL: Tactical Data Link

TDP: Tactical Data Processor

TE: Table of Equipment

TECOM: Training and Education Command

TEMP: Test and Evaluation Master Plan

TERPES: Tactical Electronic Reconnaissance Processing and Evaluation System

TFM/SFUG: Trusted Facility Manual/Security Feature User’s Guide

TGT BD: Target Board

TIBS: Tactical Intelligence Broadcast Service

TIDP: Technical Interface Design Plan

TIGER: Total Information Gateway for Enterprise Resources

TMDE: Test, Measurement and Diagnostic Equipment

TOR: Target Origination Request

TRAP: Tactical Reconnaissance and Related Applications

TRIXS: Tactical Reconnaissance Information Exchange System

TSP: Technical Support Plan

TV: Technical View

UNS: Universal Needs Statement

USMC: United States Marine Corps

USMTE: United States Message Text Format

VMFSG: Variable Message Format Subgroup

WAN: Wide Area Network

WBS: Work Breakdown Structure

WG: Working Group

WIPT: Working-level IPT

TERMINOLOGY

Accreditation: The formal declaration by the Accreditor that an Automated Information System (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards. This is also known as an Authority to Operate (ATO) (reference (I)).

AIS: Automated Information System. All information resources, either tactical or strategic, used for the collection, processing, maintenance, transmission, or dissemination of information in accordance with defined procedures. This applies to all systems connected by a LAN/WAN, (NIPRnet or SIPRnet), or stand-alone.

Application: May be a single software application or multiple software applications that are related to a single mission. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges.

Application Owner: As defined in the context of this document, this could be the Program Office of Record (POR), the Central Design Activity/Agent (CDA), or the Program Management Office (PMO).

Architecture: The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

ASP: Application Security Plan. A streamlined SSAA document that may be appropriate for less complex applications to achieve DITSCAP Certification and Accreditation.

ATO: Authority to Operate. The formal declaration by the Accreditor that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards. This is also known as Accreditation (reference (I)).

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (I)).

ATC: Authority to Connect. The formal authorization to interconnect information systems or applications within the MCEN/NMCI. This authorization is granted by the MCNOSC.

Availability: Timely, reliable access to data and information services for authorized users (reference (I)).

C4I/I: Command, Control, Communications, Computers, and Intelligence Integration. The subset of systems engineering that deals with integrating information technologies and the automated information systems or subsystems of national security systems. Within MARCORSYSCOM, C4I/I is a staff function under the Deputy Commander C4I/I (DC C4I/I) who leads Support Group 06 (SG06). SG06 consists of the C4I Systems Engineering and Integration Division (SG061), the Information Assurance and Joint Requirements Division (SG062), and the Marine Corps Tactical Systems Support Activity (MCTSSA, SG063). Systems engineering functions within the divisions of SG06 are under the line authority of the DC C4I/I, but are also accountable to the staff supervision of the Assistant Commander Engineering (ACENG) (SG05). See definition of staff supervision, paragraph 2.2.2.

CA: Certification Authority. The individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with

operating the system, coordinating the certification activities, and consolidating the final C&A package.

CCA: Clinger-Cohen Act of 1996. Law and policy requiring a systematic approach to IT acquisition, to include:

- Addressing opportunities to improve processes before investing in the IT that supports them;
- Planning for IT as an Investment;
- Considering an IA strategy for the acquisition lifecycle.

Confirmation of compliance with the CCA has been defined by the DoD as verifying compliance with the eleven (11) key items listed in the Appendix I.

The CCA has been repealed and many of its provisions reenacted at 40 U.S.C. 11101.

CCR: Communications Certification Request. The purpose of the CCR is to collect detailed application information required for evaluating and determining the application or system's overall security compliance. The CCR should be completed prior to system integration on the MCEN. The process of collecting this data is conducted onsite by application owners (Program Office of Record (POR), Central Design Activity/Agent (CDA), and/or Program Management Office (PMO). The application owner is responsible for providing information regarding their application. The CCR is used to identify the type of information required in order to accomplish the MCNOSC goals of security policy consulting and auditing.

CDA: Central Design Activity/Agent. The organization designated to design and develop software.

Certification: The comprehensive assessment of the technical and non-technical security features of a system to establish the extent to which the system meets a set of security requirements (reference (l)).

Component: One element of a larger system. A hardware component can be a device as small as a transistor or as large as a disk drive as long as it is part of a larger system. Software components are segments within a larger system. Definition from the Electronic Design Automation (EDA) Glossary of Terms.

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (reference (l)).

CRR: Certification Requirements Review. Initial meeting with the IA Team. The review is conducted in conjunction with the CA, PM, and the User Representative to negotiate and agree upon the methodology for meeting all requirements, establishing security solutions, and managing the information system security activities.

DAA: Designated Approving Authority. The official with the authority to formally assume responsibility for operating a system or network at an acceptable level of risk (reference (p)).

FedOS: Federation of Systems. A type of System-of-Systems that is managed without central authority and direction. The constituent systems of a FedOS are managed independently and have a purpose of their own. Because there is no central power or authority for direction, the participation of the constituents occurs through collaboration and cooperation to meet the objectives of the federation (reference (m)).

EIP Functional Areas include:

a) Warfighting Functional Areas:

- 1) Maneuver: 1. A movement to place ships, aircraft, or land forces in a position of advantage over the enemy. 2. A tactical exercise carried out at sea, in the air, on the ground, or on a map in imitation of war. 3. The operation of a ship, aircraft, or vehicle, to cause it to perform desired movements. 4. Employment of forces in the battlespace through movement in combination with fires to achieve a position of advantage in respect to the enemy in order to accomplish the mission (reference (c)).
- 2) Intelligence: 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (reference (c)).
- 3) Fire Support: Fires that directly support land, maritime, amphibious, and special operation forces to engage enemy forces, combat formations, and facilities in pursuit of tactical and operational objectives (reference (c)).
- 4) Logistics and Sustainment: The science of planning and carrying out the movement and maintenance of forces. In its most comprehensive sense, those aspects of military operations which deal with: a. design and development, acquisition, storage, movement, distribution, maintenance, evacuation, and disposition of materiel; b. movement, evacuation, and hospitalization of personnel; c. acquisition or construction, maintenance, operation, and disposition of facilities; and d. acquisition or furnishing of services (reference (c)).
- 5) Force Protection: Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the Joint force while degrading opportunities for the enemy (reference (c)).
- 6) Air Operations Control: The management and direction of air resources involved in the performance of the following operations: airborne, air defense (aircraft and surface-to-air missiles), airspace control, air strike/interdiction, direct air support, and search and rescue. (JINTACCS IPD (U) (Confidential) March 1984)

b) Business Management Functional Areas:

- 1) Doctrine: Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application (reference (c)).
- 2) Organization: For combat in amphibious operations, task organization of landing force units for combat, involving combinations of command, ground and aviation combat, combat support, and combat service support units for accomplishment of missions ashore. For embarkation in amphibious operations, the organization for embarkation consisting of temporary landing force task organizations established by the commander, landing force and a temporary organization of Navy forces established by the commander, amphibious task force for the purpose of simplifying planning and facilitating the execution of embarkation. For landing in amphibious operations, the specific tactical grouping of the landing force for the assault. In organization of the ground, the development of a defensive position by strengthening the natural defenses

of the terrain and by assignment of the occupying troops to specific localities (reference (c)).

- 3) Training Systems, Training Management: The systems and associated management used to impart a knowledge or skill on another system.
- 4) Material Management: The management of all items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes (reference (c)).
- 5) Leadership and Education: Functions related to the imparting of knowledge or skills as a learning process
- 6) Personnel: Functions related to the administration of human resources.
- 7) Facilities Management: The management of a real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land (reference (c)).
- 8) Financial Management. Financial management encompasses the two core processes of resource management and finance operations. Resource management is the execution of the resource management mission that includes providing advice and guidance to the commander, developing command resource requirements, identifying sources of funding, determining cost, acquiring funds, distributing and controlling funds, tracking costs and obligations, cost capturing and reimbursement procedures, and establishing a management control process. Financial operations is the execution of the Joint finance mission to provide financial advice and guidance, support of the procurement process, providing pay support, and providing disbursing support (reference (c)).

Additional Functional Areas:

- 1) Communications and Networking: The networks, communications systems, and other systems used for moving information; also the systems used to control communications networks and systems.
- 2) Command and Control: Functions that support C2 decision-making and execution performed by unit commanders by integrating the information from multiple other functional areas.

IA: Information Assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (reference (1)).

IATO: Interim Approval to Operate. Temporary approval that may be issued for up to 180 days when the requirements for full accreditation cannot be met.

IAVA: Information Assurance Vulnerability Alert. The systematic identification and assessment of vulnerabilities, and associated directing and tracking of coordinated mitigations.

Integrity: Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (1)).

Interoperability: Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Interoperability includes both technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

ITS: Information Technology System. ITS is defined as any equipment, or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, transmission, or reception of data or information by the executive agency. The term also includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Nonrepudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (reference (l)).

NSS: National Security System. Any telecommunications or information system operated by the U.S. Government, the function, operation and use of which involves intelligence activities; involves crypto logic activities related to national security; involves command and control of military forces; or involves equipment that is an integral part of a weapon or weapons system.

PMO: Program Management Office. The organization responsible for providing lifecycle management to the system/application.

PTL: Project Team Leader. The PTL is appointed by the Program Manager to head up a sub-program group, leading team efforts for a project, and representing the team within a large program. A Project Team Leader may be responsible for one or more product components. The PTL performs project functions such as planning & coordinating tasks and allocating resources, risk management, issues management, and time management. The PTL has also been known as a Project Officer.

POR: Program of Record or Program Office of Record. A program having a budget line, or the organization responsible for development of a system/application, describing automated information system acquisition programs having a budget line.

Staff Supervision: The process of advising other staff officers and individuals subordinate to the commander, of the commander's plans and policies, interpreting those plans and policies, assisting such subordinates in carrying them out, determining the extent to which they are being followed, and advising the commander thereof (reference (c)).

System: For use in this publication, the term "system" refers to a system or program. A practical definition is that a "system" will follow the complete Joint Capability Integration and Development System (JCIDS) process (reference (i)).

SOS: System of Systems. A set of different systems so connected or related as to produce results unachievable by the individual systems alone (reference (m)).

SSAA: System Security Authorization Agreement. The vehicle by which operational and security information is conveyed to the accreditation authorities (reference (l)). Templates can be accessed by requesting access on the [IA Website](#).

APPENDIX B: REFERENCES

- (a) DoD Directive 4630.5, “Interoperability, and Supportability of Information Technology (IT) and National Security Systems (NSS)”; 5 May 2004
- (b) Marine Corps Systems Command, “Command Design Team Final Deliverable”, 27 March 2001
- (c) Joint Publication 1-02, “DoD Dictionary of Military and Associated Terms”; 12 April 2001, as Amended through 23 March 2004
- (d) DoD Directive 5000.1, “The Defense Acquisition System”; 12 May 2003
- (e) DoD Instruction 5000.2, “Operation of the Defense Acquisition System”, 12 May 2003
- (f) Marine Corps Systems Command, “Enterprise Integrated Product (EIP) Configuration Management Plan (ECMP)”, 5 October 2004
- (g) CJCSI 3170.01E, “Joint Capabilities Integration and Development System”; 11 May 2005
- (h) DoD Instruction 4630.8, “Procedures for Interoperability, and Supportability of Information Technology (IT) and National Security Systems (NSS)”; 30 June 2004
- (i) CJCSI 6212.01C, “Interoperability and Supportability of Information Technology and National Security Systems”; 20 November 2003
- (j) Marine Corps Systems Command, “Enterprise Integrated Product (EIP) Master Test Plan (EMTP)”, 17 June 2005
- (k) Institute of Electrical and Electronics Engineers (IEEE) Standard 1220-1998, “IEEE Standard for Application and Management of the Systems Engineering Process”, 8 December 1998
- (l) DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP)” 30 December 1997
- (m) Krygiel, Annette J.; Behind the Wizard’s Curtain; DoD C4ISR Cooperative Research Program Publishing; July 1999
- (n) Defense Acquisition Guidebook; 8 October 2004 (non-mandatory reissue of former DoD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs)
- (o) MCO 3093.1C, “Intraoperability and Interoperability of Marine Corps Tactical C4I Systems”; 14 May 1997
- (p) DoD Directive 8500.1 Information Assurance, Oct 2002
- (q) Committee on National Security Systems (CNSS) Instruction No. 4009, “National Information Assurance (IA) Glossary”, May 2003
- (r) CJCSM 3170.01B “Operation of the Joint Capabilities Integration and Development System”; 11 May 2005
- (s) Memorandum of Agreement between Marine Corps CIO, CG MCCDC, and CG MCSC, 4 October 2002
- (t) Marine Corps System Command, “Milestone Decision Process Guide”, 30 October 2002

- (u) Marine Corps Systems Command 5200 Ser SEI/598 “Appointment As Designated Approving Authority (DAA)”, 12 July 2005
- (v) Marine Corps Doctrinal Publication (MCDP) 6, “Command and Control”, 4 October 1996

APPENDIX C: LIST OF EIP PROGRAMS

The following is a list of the 16 functional areas, used to group and manage systems that are part of the Enterprise Integrated Product (EIP). The 543 EIP systems and programs on the list that follows are as of the 1 July 2005 Configuration Status Accounting Report (CSAR). For the most current listing of this CSAR of EIP systems, please refer to the online CSAR available under MCASE at <https://mcase.usmc.mil/ispmngr/csar.aspx>.

- 1) Air Operations Control Functional Area Systems
- 2) C2 Systems Control, Networking, and Communications Functional Area Systems
- 3) Command and Control Functional Area Systems
- 4) Doctrine Functional Area Systems
- 5) Facilities Management Functional Area Systems
- 6) Financial Management Functional Area Systems
- 7) Fires Control Functional Area Systems
- 8) Force Protection Functional Area Systems
- 9) Intelligence Functional Area Systems
- 10) Leadership and Education Functional Area Systems
- 11) Logistics and Sustainment Functional Area Systems
- 12) Maneuver Functional Area Systems
- 13) Material Management Functional Area Systems
- 14) Organization Functional Area Systems
- 15) Personnel Management Functional Area Systems
- 16) Training Functional Area Systems

Project Acronym

Project Title

	Air Operations Control Function
3-D Radar	Three Dimensional Long Range Radar (AN/TPS-59(V3))
ADCP	Air Defense Communications Platform
AH-1	Cobra
AV-8B	Harrier
CAC2S	Common Aviation Command And Control System
CDLS	Communications Data Link System
CH-46	Sea Knight
CH-53	Sea Stallion
CLAWS	Complementary Low Altitude Weapons System
CWAR	Continuous Wave Acquisition Radar
DASCAS	Direct Air Support Central Airborne System
EA-6B	Prowler
F/A-18	Hornet
G/ATOR	Ground/Air Task-Oriented Radar
GCS-2000	Ground Control Station (GCS) For UAV
HELRASR	Highly Expeditionary Long Range Air Surveillance Radar
IDASC	Improved Direct Air Support Central
JRE	JTIDS Range Extension Request
JSF F-35	Joint Strike Fighter
JTIDS Terminal	Joint Tactical Information Distribution System Class 2 Terminal URC-107
KC-130	Hercules
LAAD Sustainment	Low Altitude Air Defense Sustainment
MATCALs	Marine Air Traffic Control And Landing System
MV-22	Osprey
PMS Avenger	Pedestal Mounted Stinger Avenger
Predator	Predator/Short Range Antitank Weapon
S/MR Radar	Short/Med Range Radar
TAMPS	Tactical Aircraft Mission Planning System
TAOM	Tactical Air Operations Module
TBMCS	Theater Battle Management Core Systems
TDAR	Tactical Defense Alert Radar (AN/UPS-3)
TPS-63	2-D Air Traffic Control Radar Set
UAV	Unmanned Aerial Vehicle, Pioneer
UH-1	Huey

C2 Systems Control, Networking, and Communications Function

ARC-102	HF Radio Set (AN/ARC-102)
ARC-174	HF Radio Set (AN/ARC-174)
ARC-190	HF Radio Set (AN/ARC-190)
ARC-199	HF Radio Set (AN/ARC-199)
ARC-210	Radio Set (VHF/UHF SCR) (AN/ARC-210)
ARC-94	HF Radio Set (AN/ARC-94)

Project Acronym**Project Title****C2 Systems Control, Networking, and Communications Function (continued)**

ASC-26	Heliborne Communications Group
ASQ-177	Radio Set, Airborne PLRS
AUTODIN	AUTODIN Breakout
CASC	Communications Air Support Central MRQ-12 (V)2
CGS300	Communication Gateway System 300
CGS-400	Common Ground Station 400
CIS	Communications Interface Systems
CONDOR	Command and control On-the-move Network, Digital Over-the-horizon Relay
D-DACT	Dismounted Data Automated Communications Terminal
DAGR	Defense Advanced Global Positioning System Receiver
DCS-2000	Digital Communications System 2000
DDS	Digital Data Set
DMS	Marine Corps Defense Message System
DTC	Digital Technical Control
E-LMR	Enterprise Land Mobile Radio
ECCS	Expeditionary Command and Control Suite
EPLRS	Enhanced Position Location Reporting System
GBS	Global Broadcast Service
GRC-193B	Radio Set (AN/GRC-193B (V)3)
GRC-201	Radio Set (AN/GRC-201)
GRC-210	Auxiliary Ground Radio Set (PLRS)
GRC-213	Radio Set (AN/GRC-213B)
GRC-231A	Radio Set (AN/GRC-231A (V)2)
HAVEQUICK	Radio Set (AN/GRC-171A (V)4) (HAVE QUICK II)
HFMR	High Frequency (HF) Radio
IA	Information Assurance
IRHS	Infantry Radio Headgear Set
ISR	Intra Squad Radio
JECCS	Joint Enhanced Core Communication System
JNMS	Joint Network Management System
JTRS	Joint Tactical Radio System
Local Intranet	Local Intranet
LMST	Lightweight Multiband Satellite Terminal
M-DACT	Mounted Data Automated Communications Terminal
MBMMR	Multiband Multimode Radio (AN/PRC-117F)
MCEN DW	Marine Corps Enterprise Network Data Warehouse
MCHS	Marine Common Hardware Suite
MIDS	Multifunction Information Distribution System
MRC-138B	Radio Set (AN/MRC-138B (V))
MRC-142 (DWTS)	Digital Wideband Transmission System/SMAK
MSCS	Multiple Source Correlation System (AN/TYQ-101)

Project Acronym**Project Title****C2 Systems Control, Networking, and Communications Function (continued)**

NI	Network Infrastructure
NMCI	Navy Marine Corps Intranet
PK-E	Public Key Enabling
PKI	Public Key Infrastructure
PLGR	Precision Lightweight Global Positioning System Receiver
PRC-104	HF Radio Set (AN/PRC-104)
PRC-113	Radio Set, UHF (AN/PRC-113(V)3)
PRC-150	HF Manpack Radio
PRR	Personal Role Radio
RM/T	Range Modernization and Transformation
RTU	Remote Terminal Unit
SB-22	Switchboard, Telephone, Manual (SB-22/PT)
SB-3614	Switchboard, Telephone, Automatic (SB-3614(V)TT)
SB-3865	Switching Unit, Telephone, Automatic (SB-3865)
SCT	Smart Card Technology
SINGGARS	Single Channel Ground And Airborne Radio System
SMART-T	Secure Mobile Anti-jam Reliable Tactical - Terminal
SPECTRUM XXI	SPECTRUM XXI
SPEED	System Planning, Engineering, And Evaluation Device
SPITFIRE	AN/PSC-5 Enhanced Manpack UHF Terminal
TDMS	Tactical Defense Messaging System
TDN	Tactical Data Network
THHR	Tactical Hand Held Radio
TIGER	Total Information Gateway for Enterprise Resources
TRC-170	Troposcatter Radio Set
TSC-120	HF Communication Central
TSC-85C	Ground Mobile Force (GMF) Communications Terminal (AN/TSC-85C)
TSC-93C	Ground Mobile Force (GMF) Communications Terminal (AN/TSC-93C)
TSC-96A	Fleet Satellite Communications Central
TSM	Transition Switch Module
TTC-42	Automatic Telephone Central Office Unit Level Switch
VRC-102	Radio Set (AN/VRC-102)
VRC-83	Radio Set (AN/VRC-83 (V)2)
Command and Control Function	
AAVC7A1 (RAM/RS)	Amphibious Assault Vehicle - Command Variant
C2PC	Command and Control Personal Computer
EFV-C	Expeditionary Fighting Vehicle – Command Variant
JFRG II	Joint Force Requirements Generator II
LAV-C2	Light Armored Vehicle – Command and Control Variant
MCTEEP - MT	Marine Corps Training, Exercise, and Employment Plan - Management Tools
METCAST	METCAST Client

Project Acronym**Project Title****Command and Control Function (continued)**

NFWB	Naval Flight Weather Briefer
NOWS	Night Vision Goggle Operation Weather Software
Quick Weather	Quick Weather
STACS	Staff Tasking & Collaboration System
UOC	Unit Operations Center

Doctrine Function

No Programs

Facilities Management Function

ABIS	Activity-Based Information System
FAIM	Facilities Assessment Inspection Module
FDM	Facilities Degradation Module
FED Database	Facilities Engineering Department Database
FI (Web)	Facilities Integration Website
FMCP	Facilities Management Capability Program
FPD	Facilities Project Database
FSM	Facilities Sustainment Model
iMCHAS	internet Marine Corps Housing Automated System
INFADS	Internet Navy Facility Assets Data Store
NSI	Navy Shore Installations Website
RFMIS	Rental Facilities Management Information System
SDSFIE	Spatial Data Standards For Facilities, Infrastructure And Environment

Financial Management Function

ABMS	Ammunition Budget Management System
Bond & Allotments	Bond & Allotments
CAPS-W	Computerized Accounts Payable System For Windows
CAS2NET	Contribution-Based Compensation And Appraisal System For The Internet
COBRA (SABRS)	Computer Optimized Batch Reconciliation Application
DCPS	Defense Civilian Payroll System
DIFMS	Defense Industrial Financial Management System
EAGLS	Electronic Account Government Ledger System
FACTS	Financial Air Clearance & Transportation System
FIMS II	Financial Information Management System II
Local Finance	Local Finance
MCASSP	Marine Corps Automated Settlement Sheet Process
MCX	Marine Corps Exchange
NET PAY	Net Pay Process
NOE	Notice Of Eligibility For Disability
P&R Customer Support Database	P&R Customer Support Database
P&R Portal	P&R Portal
PBAS	Program Budget Accounting System
PBDD	Program And Budgeting Documentation Database

Project Acronym**Project Title****Financial Management Function (continued)****Plant Account Plant Account**

RETPAY	Retired Process System
SABRS	Standard Accounting, Budgeting & Reporting System
SLDCADA	Standard Labor Data Collection & Distribution Application
SMARTS	SABRS Management Analysis Retrieval Tools System
SRD-1	STANFINS Re-Design One
UPL	CMC Unfunded Priority List
W2-W2C Schoolhouse	W2-W2C Schoolhouse
WINIATS	Windows Integrated Automated Travel System
WYPC	Work Year Personnel Cost

Fires Control Function

AEROS	Advanced Eye-Safe Rangefinder Observation System
AFATDS	Advanced Field Artillery Tactical Data System
ATHS II	Advanced Target Handoff System II
BCS	Battery Computer System
CLRF	Common Laser Range Finder
E/MMT	Electronic/Mechanical Meteorological Theodolite
EFSS	Expeditionary Fire Support System
Firefinder	Radar Set, Firefinder TPQ-46A
GLTD II	Ground Laser Target Designator
GWLR	Ground Weapons Locating Radar
HIMARS (USMC)	High Mobility Artillery Rocket System (USMC)
IPADS	Improved Position and Azimuth Determining System
LW155	Lightweight 155mm Howitzer
MBC	Mortar Ballistic Computer (Merlin)
MPLI	Medium Powered Laser Illuminator
MSG	Meteorological Station Group
PFED	Pocket -size Forward Entry Device
PTS-180	Precision Targeting System 180
SOFLAM	Special Operations Forces Laser Marker
SRAW Predator & SRAW MPV	Short Range Antitank Weapon Predator & Multi Purpose Variant
TCM	Trajectory Correctable Munitions
TLDHS	Target Location, Designation and Hand-Off System
TOW	Tube Launched, Optically Tracked, Wire Guided Missile Weapons System

Force Protection Function

FIRS	Family of Incident Response Systems (Formerly CBIRF)
Fly Away Communication Suite	Fly Away Communication Suite
JBTDS	Joint Biological Tactical Detection System
JSLNBCRS	Joint Service Light Nuclear, Biological, Chemical Reconnaissance System
JWARN	Joint Warning and Reporting Network

Project Acronym

Project Title

Force Protection Function (continued)

NBC Terrorism Event	NBC Terrorism Event
NBCRSP3I	Reconnaissance System Fox XM93/AI
PFDS	Proximity Fuze Defense System
TSCM	Technical Surveillance Countermeasures

Intelligence Function

CCIS	Tactical Imagery Production System
CESAS	Communications Emitter Sensing And Attacking System
CIHEP	Counterintelligence And HUMINT Equipment Program
COBRA	Coastal Battlefield Reconnaissance And Analysis
CTN	Composite Tracking Network
CTT3	Commanders' Tactical Terminal Three-Channel
DCGS-MC	Distributed Common Ground/Surface System - Marine Corps
DTAMS	Digital Terrain Analysis Mapping System
Electronic Warfare Jammer	Electronic Warfare Jammer, ULQ-19
I3 Initiatives	Integrated Intelligence and Imagery I3 Initiatives, part of GCCS-I3
IOS (V2)	Intelligence Operations Server (V2)
IOW (Intel)	Intelligence Operations Workstation - Intelligence
JDIICS-D	Joint Defense Information Infrastructure Control Systems - Deployed
JDISS	Joint Deployable Intelligence Support System
JSTARS Connectivity	Joint Surveillance Target Attack Radar System Connectivity
JTT/CIBS-M	Joint Tactical Terminal & Common Integrated Broadcast Service-Modules
MAGIS	Marine Air-Ground Intelligence System (Analysis Center, Intelligence) AN/TYQ-19(V)
MEF IAS, IOS (V2), IOW	Intelligence Analysis System Family Of Systems
MEWSS	Mobile Electronic Warfare Support System
MSIDS	MAGTF Secondary Imagery Dissemination System
RREP	Radio Reconnaissance Equipment Program
SURSS	Small Unit Remote Scouting Systems
TCAC	Technical Control Analysis Center
TEG	Tactical Exploitation Group
TERPES	Tactical Electronic Reconnaissance Processing And Evaluation System
THSE	Tactical Hydrographic Survey Equipment
TPCS -MPC	Team Portable Collection System Multi-Platform Capable
TPC	Topographic Production Capability
TROJAN LITE	TROJAN SPIRIT Lightweight Integrated Telecommunications Equipment
TROJAN SPIRIT	TROJAN Special Purpose Integrated Remote Intelligence Terminals
TRSS	Tactical Remote Sensor Systems
TUGV	Tactical Unmanned Ground Vehicle
TVRSTA	Tactical Vehicle Reconnaissance Surveillance and Target Acquisition Capability

Leadership and Education Function

DL	Distance Learning Program
----	---------------------------

Project Acronym**Project Title****Leadership and Education Function (continued)**

JCDE FB Joint Concept Development and Experimentation Force Builder
TDSS Tactical Decision-making Simulation System

Logistics and Sustainment Function

AIS Aeronautical Information System
AL Autonomic Logistics
AMRR Aircraft Material Readiness Report
AMS-TAC Automated Manifest System-Tactical
ARS Advanced Radiographic System
ATICTS Automated Tool Inventory Control Tracking System
ATLASS I Asset Tracking Logistics And Supply System I
BARBARA SIRS Broadened Arrangement Of Resources From A Basic Accessory Relocation Application - Supply Issue And Recovery System 2000
BCS3 Battle Command Sustainment Support System
CALMS Computer Assisted Load Manifesting System (CALMS)
CALTECS Computer Assisted Logistics And Test Equipment Calibration System
CAMIS Commercial Activities Management Information System
CAV II (Training) Commercial Asset Visibility 2 (Training)
CCS Command Core System
CLC2S Common Logistics Command and Control System
CMIS WEB Configuration Management Information System
CMOS Cargo Movement Operations System
Contracts Directorate Document Control System Contracts Directorate Document Control System
CPARS Contractor Performance Assessment Reporting System
CRS Cataloging Reengineering System
CSSE SDE/Data Warehousing CSSE Shared Data Environment
Data Entry Data Entry
DMLSS Defense Medical Logistics Standard System
DMMS Depot Maintenance
DPAS Designer Defense Property Accountability System Report Designer
DPAS Viewer Defense Property Accountability System Report Viewer
DSS Distribution Standard System
DSSC Direct Support Stock Control Subsystem
DTOD Defense Table Of Official Distances
EPOS Electronic Point Of Sale
EPPG Electronic Project Procurement Generator
ERP Essex Replacement Program
ETPS Electronic Technical Publication System
Field MIMMS Field Maintenance Subsystem (MIMMS)
Fuels Manager Fuels Manager
GATES Global Air Transportation Execution System
GCSS-MC Global Combat Support System
GDSS Global Decision Support System
GFM Global Freight Management System

Project Acronym**Project Title****Logistics and Sustainment Function (continued)**

GME (FA)	Garrison Mobile Equipment Fleet Anywhere
GOPAX	Groups Operational Passenger System
GTN	Global Transportation Network
GUI Logistics On-Line Application	Graphical User Interface Logistics On-Line Application
Hazardous Materials Awareness	Hazardous Materials Awareness
Hazardous Materials Incident Commander	Hazardous Materials Incident Commander
Hazardous Materials Operations	Hazardous Materials Operations
HICS	Hazardous Material Information Control System
HMMS	Hazardous Materials Management
HMMWVA2	High Mobility Multipurpose Wheeled Vehicle A2 Series
HSMS	Hazardous Substance Management System
IA MERIT	Investment Advisor - MERIT
IBS	Integrated Booking System
ICF SS03	Inventory Control Forecasting, Subsystem Of ICP
ICODES	Integrated Computerized Deployment System, part of MAGTF LOGAIS
ICP	Inventory Control Point
IFAV	Interim Fast Attack Vehicle
IMA NALCOMIS	IMA Naval Aviation Logistics Command Information System
Integrity	Integrity
IRRIS	Intelligent Road/Rail Information Server
Item Applications On-Line	Item Applications On-Line
ITEMAPPS	Item Applications
ITV	Internally Transportable Vehicle
JCALs	Joint Computer-Aided Acquisition and Logistics Support
JDSR	Joint Distance Support and Response
JEDMICS PC	Joint Engineering Data Management Information Control System - PC
JEDMICS	Joint Engineering Data Management Information Control System
JLWI	Joint Logistics Warfighting Initiative
JTAV	Joint Tactical Asset Visibility
KME	Knowledge Management Enterprise
Lakes Helper	Lakes Helper
LBIV-II	Logistics Bases Inventory Visibility Phase II
LINK	Logistics Information Network
LMIS	Logistics Management Information System
LOGS	Local Logistics
MAGTF LOGAIS	Marine Air Ground Task Force Logistics Automated Information System
MAP	Maintenance Automated Program
MAXIMO	COTS Software for Facilities Management Capability Program
MC DoD Automatic Addressing Directory	Marine Corps Department Of Defense Automatic Addressing Directory
MCDRS	Maintenance Center Document Retrieval System
MCDSS	Materiel Capability Decision Support System

Project Acronym**Project Title****Logistics and Sustainment Function (continued)**

MDSS II	MAGTF Deployment Support System II (MDSS II), part of MAGTF LOGAIS
MEDALS	Military Engineering Data Asset Locator System
MERIT	Marine Corps Equipment Readiness Information Tool
MFMP	Material Forecast Management Plan
MHIF-OL	Master Header Inventory File On-Line
MICAPS	Marine Corps Interactive Computer Aided Provisioning System
MIMMS	Marine Corps Integrated Maintenance Management System (MIMMS)
MOWASP	Mechanization Of Warehousing And Shipment Processing
MRP	Material Returns Program
MUMMS SS04	Stores Accounting System
MUMMS	Marine Corps Unified Material Management System
NAFI	Navy Air Force Interface
NALCOMIS	Naval Aviation Logistics Command Management Information System
NECO	Navy Electronic Commerce On-Line
NFIRS	National Fire Incident Reporting System
NIMMS	NAVAIR Industrial Materiel Management System
NTCSS IBS	NTCSS Integrated Barcode System
OIMA NALCOMIS	Optimized IMA Naval Aviation Logistics Command Information System
OOMA NALCOMIS	Optimized OMA Naval Aviation Logistics Command Information System
PCMIMMS	Personal Computer-Marine Corps Integrated Maint. Management System
PCMISCO	Personal Computer-Maintenance Information Systems Coordination Office
PRF-FOLLOW UP	Inventory Control Project Requirements File Follow-Up Subsystem of ICP
PTOPS	Pilot Transportation Operational Personal Property System
QIR	Quality Inspection Reporting
REP REVIEW	Inventory Control Replenishment Review Subsystem of ICP
ROLMS	Retail Ordnance Logistics Management System
R-SUPPLY	Relational Supply System
Safe-Range	Safe-Range
SAS	Set Assembly System
SASSY	Supported Activities Supply System (SASSY)
SCS	Stock Control System (SCS)
Shipping MATS 1.2.0	Shipping MATS 1.2.0
SL 1-2/1-3 On Line	Stock List 1-2/1-3 - Online
SS07 MUMMS (DSSC)	MUMMS Direct Support Stock Control System
SS10 MUMMS (Prov)	MUMMS Provisioning
SL 1-2/1-3 PC	Stock List 1-2/1-3 - PC
S-L	Seaway-Loggy
SMOL	ServMart On-Line
STAIRS	Standard Automated Inventory And Referral System
STORES NT	Subsistence Total Order And Receipt Electronic System NT

Project Acronym Project Title

Logistics and Sustainment Function (continued)

TAMIS-R Stratification	Total Ammunition Management Information System-Redesigned Stratification
TC-AIMS	Transportation Coordinators Automated Information For Movement System
TC-AIMS II	Transportation Coordinators Automated Information For Movement System II
TDMS	Technical Data Management System
TETS	Third Echelon Test System
TIMA	Tool and Inventory Management Application
TMDIS21	Test Measurement, Diagnostic Information System (For The 21st Century)
TMIP-M	Theater Medical Information Program (Maritime)
TMS Freight Sys	Transportation Voucher
TMS	Transportation Management System
UADPS	Uniform Automated Data Processing System
VLIPS	Visual Logistics Information Processing System
WISE	World Wide Integrated Logistics Capability Interim Supply and Maintenance Evaluation System
WRS	War Reserve System

Maneuver Function

AAVP7A1	Amphibious Assault Vehicle, Personnel
ABV	Assault Breaching Vehicle (ABV)
EFV	Expeditionary Fighting Vehicle
IOS (V1)	Intelligence Operations Server (V1)
IOW (Ops)	Intelligence Operations Workstation - Operations
LAV-AAS	Light Armored Vehicle Advanced Antitank System
MCTIS / CID	Mounted Cooperative Target Identification System (MCTIS) / Combat Identification (CID)
SURC	Small Unit Riverine Craft

Material Management Function

Albany Publishing System	Albany Publishing System
ASCP	Automated Security Control Program
BelManage	BelMange
CAPS	Command Automated Program Information System
CAV II	Commercial Asset Visibility II
CMCPB	CMC Preparation Briefs
CMIS/MEARS	Configuration Management Information System/ Multi-User Electronic Change Proposal Automated Review System
Data Elements	Data Elements
DAWIA Reporting Program	Defense Acquisition Workforce Improvement Act Reporting Program
Department Of The Army Electronic Tech Manual	Department Of The Army Electronic Tech Manual
DSAMS	Defense Security Assistance Management System
FIMS	Fleet Imaging Management System

Project Acronym**Project Title****Material Management Function (continued)**

FTP	File Transfer Program
H Series ACODP Handbook	H Series Allied Codification Publication (ACodP) Handbook
IDE Increment 0	Command Integrated Digital Environment - Increment 0
IDE Increment 1	Command Integrated Digital Environment - Increment 1
IRS	Inquiry Response System
JATDI	Joint Aviation Technical Data Integration
JDEP	Joint Distributed Engineering Plant
JTMs	Joint Technical Manuals
K21	Knowledge For Acquisition In The 21st Century
LDR	Logistics Data Repository
MAARS II	Marine Ammunition Accounting and Reporting System
MAGTF	Marine Air Ground Task Force
MCASE	Marine Corps Architecture Support Environment
MCATS	Maintenance Center Asset Tracking System
MCATS	Marine Corps Action Tracking System
MCEFS	Marine Corps Electronic Forms System
MCPDS	Marine Corps Publications Distribution System
MCS D	Marine Corps System Division
MCSELMS	Marine Corps Software Enterprise License Management System
MERS	Marine Expeditionary Rifle Squad
MRP	MRP Reports Application
ODI-RMS	Optical Digital Imaging Records Management System
OIS	Naval Ordnance Information System
P2ADS	Pollution Prevention Annual Data Summary
PA	Paperless Acquisition
PDREP	Product Data reporting Evaluation Program
Permissions Management	Permissions Management
PIB	POM Initiative Builder
PMRS	Procurement Management Reporting System
Property Accountability	Property Accountability
SCRT	Standard Contract Reconciliation Tool
SPS	Standard Procurement System
STOIC	Science And Technology Operation Information Center
STRATIS	Storage Retrieval Asset Tracking Information System
TOPS	Transportation Operational Personal Property System
TPL	Technical Publications Library Program
TRACKER	Tracker
UDR	Universal Data Repository
ULAS	Unit Level Ammunition Status
VPMS	Virtual Program Management System
WAW	Wide Area Work Flow
WAW-RA	Wide Area Work Flow-Receipts And Acceptance

Project Acronym**Project Title****Material Management Function (continued)**

Weapons Serial Tracking System Weapons Serial Tracking System
WSS Warehouse Support System

Organization Function

TFDW Total Force Data Warehouse
TFSMS Total Force Structure Management System

Personnel Function

ACRS Automated Career Retention System
AFRS Automated Fitness Report System
ALMRS Automated Leads Management Reporting System
ARMS Automated Recruit Management System
AUTH STR&MAN Authorization Strength & Manning Levels
BNA By Name Assignment
BUPERS Bureau Of Naval Personnel
C123M Class I / II / III Maintenance
CCLD/CWDA Civilian Career and Leadership Development/Civilian Workforce
Development Application
CHCSII Composite Healthcare System II
CSU Civilian Servicing Unit Application
DCIPS Defense Casualty Information Processing System
DEERS Defense Enrollment Eligibility Reporting System
DENCAS Dental Common Access System
DENCAS(R) Dental Common Access System (Remote)
DENMIS Dental Management Information System
Deserter Process Deserter Process
DIMHRS Def Integrated Military Human Resources System
DPRIS Defense Personnel Records Imaging System
DSRTR Deserter
DTAS Deployable Theater Accountability Software
DTS Defense Travel System
EAM Enlisted Assignment Model
EFMP Exceptional Family Member Program
ESGM Enlisted Staffing Goal Model
EQual Explosive Safety Qualification Certification
GOSA General Officer Slating Application
HMF Headquarters Master File
JPAS Joint Personnel Adjudication System
Local Manpower Local Manpower
Locator Locator
M4L Marine For Life
Mailgram Model Mailgram Model
MASS Manpower Assignment Support System
MCEAS Marine Forces Enlisted Administrative Separation System

Project Acronym

Project Title

Personnel Function (continued)

MCMEDS	Marine Corps Medical Entitlements Data System
MCMODS (ODSE)	Marine Corps Manpower Operational Data Store
MCMPS	Marine Corps Mobilization Planning System
MCRISS-RS	Marine Corps Recruiting Information Support System For Recruiting Stations
MCTFS	Marine Corps Total Force System
MDCPDS	Modern Defense Civilian Personnel Data System
MEM	Marine Equity Model
MIPS (UD/MIPS)	Marine Integrated Personnel System (MIPS) Marine Integrated Logistics System (MILOGS)
MLP	Manning Level Process
MMAS	Manpower Mobilization Assignment System
MMS	Manpower Management System
MODELS	Manpower Models
NCMIS	Navy College Management Information System
ODV	Operation Determined Vigilance
OLDS	On-Line Diary System
OMM	Officer Mobilization Model
OPUS	Officer Planning and Utility System
ORG	Officer Rate Generator
OSGM	Officer Staffing Goal Model
PCS HIST	Permanent Change Of Station History
PES	Performance Evaluation System
PPP	Promotion Planning Process
PREPAS	PREPAS
RCCPDS	Reserve Component Common Personnel Data System
RDM	Recruit Distribution Model
RECRPTS	Recurring Reports
Recruit Admin	Recruit Admin
Recruit Evaluation	Recruit Evaluation
Recruit Labels	Recruit Labels
REPS	Reserve Enlisted Planning System
ROWS	Marine Forces Reserve Order Writing System
RSGM	Reserve Staffing Goal Model
RSM	Reserve Staffing Model
SDI	Smart Dental Information
STATS	Statistics Reports
TFAS	Total Force Administration System
TFPM	Target Force Planning Model
TFRS	Total Force Retention System
TMR	Table Of Manpower Requirements
TRIMEP	Tri-Service Medical Evaluation Program For Aviation Physical Waiver Requests

Project Acronym

Project Title

Personnel Function (continued)

USMC Recruit Manifest	USMC Recruit Manifest
VEF Extract	VEF Extract
VMET	Verification Of Military Experience And Training System
YGSS	Year Group Steady State

Training Function

AMTCS-ICW	Aviation Maintenance Training Continuum System (AMTCS) Support Software Suite for Interactive Courseware (ICW)
ATRRS	Army Training Requirements And Resources System
CACCTUS	Combined Arms Command and Control Training Upgrade System
CLASS	Closed Loop Artillery Simulation System
CVTS	Combat Vehicle Training System
DAU	Defense Acquisition University
Driver/Operator Pumper	Driver/Operator Pumper
EFV Training	Expeditionary Fighting Vehicle Training System
First Aid First Responder Training	First Aid First Responder Training
IMTS	Improved Moving Target Simulator
ISMT/ISMT-E	Indoor Simulated Marksmanship Trainer (ISMT)/ISMT - Enhanced (ISMT-E)
Logbook	Logbook
LOMAH	Location of Miss and Hit
MCDL	Marine Corps Distance Learning
MEPCOM TRANS	Military Entrance Processing Command Transportation
MILES 2000	Multiple Integrated Laser Engagement System 2000
MOSTAS	Marine Officer Specialty Training Allocation System
MTWS	MAGTF Tactical Warfare Simulation
NITRAS WEB	Navy Integrated Training Resources Administration System
OTA	Oracle Training Administration
PGTS	Precision Gunnery Training System
PITS	Portable Infantry Target System
RETS	Remoted Target System
RIS	Range Instrumentation Systems
SREIS	Situation Report Executive Information System
TIMS	TECOM Integrated Management System
TRRMS	Training Requirements And Resource Management System

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: C4I INTEGRATION BOARD AND SE&I DIVISION CHARTERS

The following pages contain the C4I Integration Board Charter. The document was approved on 28 January 2003. The Operations Division under the Deputy Commander, C4I Integration, holds the original copy, signed by all parties identified on the final page. Starting on page D-5 is the SE&I Team Charter, approved 21 June 2003.

Team Name:	Level of Team:
Command, Control, Communications, Computers, Surveillance, and Reconnaissance (C4ISR) Integration	Management Team
Team Mission	
<p><i>Ensure delivery and sustainment of a <u>superior</u> integrated, and interoperable Enterprise C4ISR capability to the operating forces and supporting establishments. * (Includes all C4ISR systems that connect in any way with DoD data networks both tactical and non tactical. Does not include electronics that do not connect in any way to any other systems. Interoperability: (1) The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services, units, or forces and to use the services so exchanged to enable them to operate effectively together. (2) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. Integration: The stage of system development and demonstration that applies to systems that have yet to achieve system level design maturity as demonstrated by the integration of components at the system level in relevant environments.)</i></p>	
Team Goals/Objectives/Metrics	
<p>Our team will collaborate to make value added integration decisions.</p> <ul style="list-style-type: none"> - Utilize the Functional Integration Team (FIT) construct within the processes. - Establish and agree to the process for the resolution of Inter/Intra PG issues. (3rd Qtr FY 03) - Establish and agree to the process for the resolution of external interoperability issues for Marine Corps positions. (4th Qtr FY 03) <p><i>(metrics: SIE tests, JITC tests, OT/DT tests, PQDR resolutions)</i></p> <p>Our team will manage the configuration of the Enterprise Architecture.</p> <ul style="list-style-type: none"> - Utilize the FIT construct within the processes. - Establish and agree to the process for Configuration Management. <p><i>(metrics: produce an accurate Configuration Status Accounting Report (CSAR), Qtrly)</i></p> <p>Our team will assist in the achievement of successful Milestone Decisions/Post Production Block Upgrades in respect to interoperability and integration.</p> <ul style="list-style-type: none"> - Utilize the FIT construct within the processes. - Assist PG in preparation of a system's C4ISP assuring C4ISP work is completed prior to 90% of upcoming milestones. - Ensure IA objectives for AIS/IT systems (IAW CCA) are completed prior to 90% of upcoming milestones. <p><i>(metrics: Percentage of approved C4ISPs in ratio to number required, time to process them. Percentage of approved SSAAs, ASPs, ATOs, and IATOs in ratio to number required, time to process them.)</i></p> <p>Our team will ensure proactive conformance to interoperability standards.</p> <ul style="list-style-type: none"> - Utilize the FIT construct within the processes. 	

- Establish and agree to the process for the development of USMC positions on Joint Interoperability Standards.
- Utilize the Fit construct within the processes.
- Provide tailored interoperability specifications.
- Establish and agree to the Enterprise Integrated Process (EIP).

(metrics: percentage of systems that successfully participate in the EIP Assessment.)

Our team will embrace, follow, and foster system engineering standards and best practices.

- Utilize the FIT construct within the processes.
- Provide guidelines for implementing system engineering and best practices on all programs.
- Provide coordinated tailorable interoperability specification for implementation tailored system architecture products.

(metrics: percentage of C4I/I programs implementing IEEE 1220)

Customers/Stakeholders

Customers:

PGD 10 –16

Independent PM's

DRPM AAAV

Operating Forces

Supporting Establishments

Stakeholders:

HQMC, MCCDC, ASN RDA, DISA, TECOM, MCOTEA, ONI, MATCOM, JFCOM, JITC, NAVCOMPT

Team Products/Services

An Enterprise architecture.

Documentation for all processes defined in this charter.

Approved documentation resulting from the process definition. (e.g. C4ISP's SSAA's, ASP's, ATO's, IATO's, CMP, TSP's)

System engineering guidelines.

Aggregate EIP results

Team Membership by Discipline/Organization/Function

Name	Organization	Function
Mr. Hobart	C4II	Team Leader
Col Albano	MCTSSA	Commanding Officer
Ms Wasielewski	C4II	C4I Integration Support
Major Wiktorek	C4II	C4I Integration Support
Ms Ashby	C4II	C4I Integration Support
Mr. Smith	C4II	Director, SE&I
Mr. Davis	C4II	Director, IA
Mr. Raton	PG 10	Acting Lead Eng
Maj Eads	PG 11	Acting Lead Eng

Col Allen	PG 12	PGD, MAGTF C4ISR
Mr. Parker	PG 13	Lead Eng
Mr. Lerner	PG 14	Lead Eng
Ms. Redfern	PG 15	Lead Eng
Mr. Leitner	PG 16	Lead Eng
Mr. Robert Tekampe	NGIT	Program Manager
Mr. W. K. Tritchler	MITRE	Senior Engineer for external Interoperability issues
LtCol H. Oldland	DRPM AAA	C4I Division Director/APM(C)
I/II MEF Liaison Officers	I/II MEF	Adhoc membership
PM LAV, PM LW155, PM TRA		As req'd

Team Leader Responsibility

- Conduct C4I Integration Meetings monthly beginning 1st quarter 2003. (continuation of existing forum)
- Conduct Target Board Meeting quarterly beginning 1st quarter 2003. (continuation of existing forum)
- Document, train, and institutionalize all processes developed.
- Executive Management of SE&I, IA Divisions and MCTSSA.
- Leads C4I Integration Team (i.e., single integrated air picture; single integrated ground picture)
- Brings together the appropriate Product Strategy Team Leaders for integration decision making
- Transforms MCTSSA into a Systems Integration Environment
- Manages Support Staff to include: C4I Integration Support Team

Authority/Accountability/Boundaries

Federal Acquisition Regulations (FAR)
DoD 5000 series and related documents
CIO Roles and Responsibilities
Clinger Cohen Act

Review and Approval Process

Date of Approval: 28 Jan 03 (Will be reviewed semi-annually)

Approved

Submitted by Signature on File
Submitted

Signature on File
Commanding General
Marine Corps System Command

Deputy Commander C4I Integration
Marine Corps System Command

Name	Org	Function	Signature
Mr. Hobart	C4II	Team Leader	Signatures on File
Col Albano	MCTSSA	Commanding Officer	
Carol Wasielewski	C4II	Operations Officer	
Major Wiktorek	C4II	C4I Integration Support	
Ms Ashby	C4II	C4I Integration Support	
Mr. Smith	C4II	Director, SE&I	
Mr. Davis	C4II	Director, IA	
Mr. Raton	PG 10	Acting Lead Eng	
Maj Eads	PG 11	Acting Lead Eng	
Col Allen	PG 12	PGD, MAGTF C4ISR	
Mr. Parker	PG 13	Lead Eng	
Mr. Lerner	PG 14	Lead Eng	
Ms. Redfern	PG 15	Lead Eng	
Mr. Leitner	PG 16	Lead Eng	
LtCol H. Oldland	DRPM AAA	C4I Division Director/APM(C)	

Team Name	Level of Team
Systems Engineering and Integration (SE&I) Division	Engineering Team
Team Mission	
<i>Support command-level oversight for Marine Corps Systems Command (MARCORSYSCOM) of C4ISR system engineering and integration within the command; lead the team of C4ISR system engineering professionals in the instantiation and maintenance of the Marine Corps C4ISR Enterprise Architecture.</i>	
Team Goals and Objectives	

1. *Goal*

- *Objective*

- *Success Criteria/Products (Delivery Dates)*

1. Establish and execute the processes necessary to manage interoperability of C4ISR systems across MARCORSYSCOM using a command-wide strategy of centralized planning and decentralized execution.

- Develop a comprehensive system view of the C4ISR architecture for the USMC Enterprise.
 - Marine Corps Integration Architecture Pictures for 2004 (complete, 2006 (TBD), 2015 (31 Dec 02).
- Provide storage for the USMC enterprise-wide system architectural data in a user-friendly database.
 - Marine Systems and Technical Architecture Repository (MSTAR), (validated per MS Review, reported monthly; validation per functional area, TBD).
- Provide additional architectural services to USMC Enterprise-wide users.
 - MSTAR remote access via internet (availability reported monthly).
- Deliver interoperability and interface requirements to MARCORSYSCOM and MARCORSYSCOM-supported product teams.
 - Operational and system architectural views/C4I Support Plans (C4ISP), (percent completed vs. required for internal), (Configuration Status Audit Report [CSAR] provided quarterly).
- Define the MARCORSYSCOM Enterprise Integrated Product (EIP) and maintain configuration control of the interoperability and interface specifications of that product.
 - EIP letter of instruction, configuration management plan, configuration status report (per program schedule, reported bi-weekly).
- Assess the performance of the Enterprise Integrated Product and report the results to the Commanding General.
 - EIP assessment report (30 Sep 03).
- Provide a forum for resolution of interoperability and integration issues among MARCORSYSCOM and MARCORSYSCOM-supported product teams and between MARCORSYSCOM and MARCORSYSCOM-supported product teams and external programs.
 - On-call assessments (when occurring, reported monthly).
 - Target board issue resolution (Target Board IPT reports quarterly).
 - Interoperability working group reports (quarterly).
 - Configuration management board issue resolution (quarterly).

- Provide staff cognizance to the Commanding general for the Systems Integration Environment.
 - SE&I maintenance and upgrade plan and budget (program schedule bi-weekly).
 - JDEP maintenance and operations planning (program schedule bi-weekly).
2. Establish and execute the processes necessary to ensure that MARCORSYSCOM C4ISR systems interoperate with the appropriate systems of the other Services and joint commanders.
 - Manage MARCORSYSCOM participation in working groups whose purpose is to define joint interoperability standards.
 - Plan to support MCEB working groups (provide after action results).
 - Plan to support NCES-family working groups (provide after action results).
 - Deliver requirements for joint interoperability standards to MARCORSYSCOM and MARCORSYSCOM-supported product teams.
 - Technical architectural views (when occurring, reported monthly).
 - Joint Interoperability Test Center (JITC) test reports (number received reported monthly).
 - Provide storage for the USMC enterprise-wide technical architectural data in a user-friendly database.
 - MSTAR (continuous)
 3. Provide programmatic representation for USMC technical requirements to external program offices and other agencies, when the product is not otherwise assigned to a Marine Corps product group, independent program manager, or direct reporting program manager.
 - Provide liaison with developers of joint programs and programs of other Services to represent USMC system and technical requirements, when such liaison is not accomplished by project teams. (Number of external/joint C4ISPs reviewed reported monthly.)
 - Joint Strike Fighter C4ISR architecture and C4ISP.
 - Osprey V-22 C4ISR architecture and C4ISP.
 - Lead the USMC integration representation to the US Navy to ensure that the needs of the landing forces are met when operating afloat.
 - D-30 process reports (number of MAGTF Afloat Baseline [MAB] systems installed at ship delivery date).
 - New construction system specifications (number of MAB systems installed at ship delivery date).
 - Integration issue reports (when occurring).
 - Military Capabilities Packages working group products (budgets, plans, architectural views).
 - Lead the USMC representation the Joint Warrior Interoperability Demonstrations and plan effectively for transition of these technology products into acquisition programs.
 - JWID after-action reports (FY annual).
 - Successful transitions of C4ISR technology into acquisition programs (When occurring).

- Lead the MARCORSYSCOM representation to MCCDC working groups developing future warfighting concepts, including Marine Corps Warfighting Laboratory experiments and the various working groups of the Expeditionary Warfare Development System.
 - Working groups reports (when occurring).
 - Adjustments to architectural products (when occurring).
 - Lead the USMC representation to the designated Future Naval Capability initiatives under ONR and plan effectively for transition of these technology products into acquisition programs.
 - Number of relevant USMC-related technology projects in ONR FNCs (Tri-annual).
 - Successful transitions of C4ISR technology into acquisition programs (when occurring).
4. Establish and execute processes for providing direct support to MARCORSYSCOM and MARCORSYSCOM-supported product Teams.
 - *(Objectives TBD)*
 5. Provide on-call support to the Commanding General and the Deputy Commander for C4I Integration on emergent topics (when occurring).

Customers/Stakeholders
Commanding General MARCORSYSCOM Deputy Commander C4ISR Integration MARCORSYSCOM PGDs and PMs, CO MCTSSA MARCORSYSCOM and MARCORSYSCOM-supported Product Teams.
MCCDC EFDS Division, MCCDC action officers HQMC (CIO, Advocates) MCOTEA Operating Force/MEF/BPS G-6s
JCS, OSD, ASN Engineering Agencies, ONR
Other SYSCOMs

Team Membership by Discipline/Organization/Function			
	Name	Organization	Function
	Mr. J. Kevin Smith	C4I/I SE&I	Director, SE&I
	Mr. Al Taschner	SE&ISC	Director, SE&ISD
	Maj Roger Roland	SE&ISD	Dep Director, SE&ISD
	Mr. Robert Tekampe	NGIT	NGIT Team Manager
	Maj John Gambrino	C4I/I SE&I	Assessment Section Head
	Mr. Marty Marbach	NGIT	Assessments Support
	Mr. Ronn Johnson	OSEC	Assessments Support
	Maj Allen Johnson	C4I/I SE&I	JNC Team Lead
	Maj Gerald Bloomfield	SE&ISD	SIE Arch & Eng Branch Head
	Capt Ferrando	C4I/I SE&I	EIP Team Lead
	Mr. Dennis Moore	NAWC	EIP/JDEP
	Mr. Joe Johnson	C4I/I SE&I	Technical Section Head
	Mr. David Matthews	C4I/I SE&I	Technical Section
	Mr. Earl Connally	SE&ISD	Interoperability Branch Head
	Mr. Eldon Perkins	NGIT	Technical Section Support
	Mr. Vic Cole	NGIT	NCES Technical Support
	Mr. James Mayers	C4I/I SE&I	JNC Technical Lead
	LTCOL Paul Guerra	MCTSSA	LNO to SPAWARSSYSCOM
	CDR Irma Sityar	SPAWARSSYSCOM	LNO from SPAWARSSYSCOM
	LTCOL Chris Daniels	C4I/I SE&I	Joint Programs LNO
	Mr. Mike Cajohn	NGIT	USA/USAF LNO and Misc EMW Technical Support (JWID, KSA FNC, BFC2/FORCENET MCP)
	Capt Samuel Laboy	C4I/I SE&I	Naval Integration Team Lead
	MSgt Wagner	C4I/I SE&I	Naval Integration Section
	Mr. Hugh Carter	NGIT	Naval Integration Section
	Capt Gaines	C4I/I SE&I	EMW Integration Section Team Lead
	Mr. Jack Hughes	NGIT	EMW Technical Support (MCWL, LC FNC, Seabasing FNC, Tier 3 Relay)
	Mr. Ron Smith	NGIT	Acting Head Architecture and DSS Team
	Mr. Chris Christy	NGIT	Architectures Technical Support
	Mr. Cliff Hester	NGIT	CDD Team Leader
	Mr. Paul Terebesi	NGIT	DSS Technical Support
	ADJUNCT MEMBERS		
	Ms. Carol Wasielewski	C4I/I OPS	Operations Division Head
	Maj Brian Wiktorek	C4I/I OPS	Operations Officer
	Mr. Michael Davis	C4I/I IA	Information Assurance Division Head
	Ms. Pati Murphy	NGIT	Administrative Support

Team Leader Responsibility
Establishing Priorities. Assigning resources. Coordination with external agencies at the senior management level. Facilitating cross-team synergy. Technical review of products. Representation to higher authority.
Authority/Accountability/Boundaries
DoD 5000 series and successors. CJCSI 4630.5 and 4630.8. C4IST architecture framework. Joint Technical Architecture. Levels of Information systems Interoperability LISI Joint Vision 2020 Implementation Master Plan USMC C4 Campaign Plan IEEE Standard 1220 Series Marine Corps Order 3093 Series MARCORSYSCOM Order 3093 Series MQMC/MCCDC/MCSC MOA CIO Roles and Responsibilities
Review and Approval Process
Date of Approval: <u> 21 Jun 03 </u> (Will be reviewed semi-annually)
Submitted by _____ [J. K. Smith, Acting Director, SE&I Division]
Approved by _____ [R. L. Hobart, Dep Cmdr, C4I Integration Directorate]
Signatures on File

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E: EIP TARGET BOARD CHARTER & PROCESS

Appendix E provides the charter and process for the Enterprise Integrated Product (EIP) Target Board.

E.1 Background.

The Enterprise Integrated Product (EIP) Target Board Process was developed to assist Marine Corps Product Group Directors/Program Managers/Product Team Leaders in the initiation, development and execution of C4I interoperability and integration targets. DoD Directives 5000.1, 4630.5, DoD Instructions 5000.2, 4630.8, and the Defense Acquisition Guidebook (DAG), references (d), (a), (e), (h), and (n) establish the DoD's disciplined management approach for acquiring C4I systems and materiel that satisfy the operational user's needs. These references apply to major and non-major defense acquisition programs. CJCSI 3170.01 and 6212.01, references (g) and (i) establish the certification of interoperability requirements for Information Support Plans (ISP) and the policies and procedures for the Joint Capabilities Integration and Development System (JCIDS). MCO 3093.1, reference (o) establishes Marine Corps command and control systems interoperability policy and implementation procedures to ensure the interoperability of Marine Corps information systems with interfacing DoD, Joint, and other Marine Corps C4I systems.

Too often in the past, the focus for acquiring IT systems was accomplished without the necessary regard to the larger context of how the systems will actually be used and how the systems would be supported throughout its life cycle. To achieve information superiority as specifically required by the DAG, reference (n), the Deputy Commander, C4I Integration, has been tasked to enforce the use of sound system engineering principles and practices across all elements of MARCORSSYSCOM. DoDD 5000.1, reference (d) states that "Acquisition managers shall provide U.S. Forces with systems and families of systems that are secure, reliable, interoperable, compatible with the electromagnetic spectrum environment, and able to communicate across a universal information technology infrastructure, including NSS, consisting of data, information, processes, organizational interactions, skills, analytical expertise, other systems, networks, and information exchange capabilities". As such, MARCORSSYSCOM must focus on developing a synergistic, product-centric approach across all of the Product Group Directorates (PGDs). This product-centric approach is necessary to create a controlled, secure, interoperable and integrated, enterprise-wide C4ISR federation-of-systems that supports the MAGTF commander in a Joint environment.

E.2 EIP Target Board Charter

a. **Purpose:** This charter establishes the EIP Target Board, which shall function under the authority of the Deputy Commander, C4I Integration, MARCORSSYSCOM. The Target Board shall assist the Deputy Commander with achieving information superiority across the MAGTF and is responsible for the oversight and management of interoperability and integration "targets". Targets are system-level issues, which pose a potential impact to the Marine Corps Enterprise Architecture. Targets will involve system interoperability and integration issues between systems that are managed by different Product Group Directors (PGDs), which cannot be resolved at lower echelons. Targets may also include system interface issues between Marine Corps systems and systems of other Services and external agencies, as well as other significant system interface and integration issues that require the concurrence of the Commanding General, MARCORSSYSCOM.

b. Objectives: The Deputy Commander, C4I Integration will work with the MARCORSYSCOM PGDs to develop an interoperable and integrated Enterprise-wide C4I federation-of-systems. The Marine Corps Enterprise C4I systems architecture shall consist of a collection of subsystems (hardware and software) designed to automate the processes associated with one or more of the sixteen functional areas as identified in Section 3.2. These subsystems are the sources of the data shared between Marine Corps organizations and operational facilities. By using common computer hardware, fully integrated software, common data meanings, and approved Joint standards and interfaces with compatible implementations, Marine Corps C4I systems are better positioned, and will have the capability for seamless interoperability regardless of the functional area(s) they support.

c. Membership:

- Deputy Commander for C4I Integration, MARCORSYSCOM (Chairman)
- MARCORSYSCOM PGD 10
- MARCORSYSCOM PGD 11
- MARCORSYSCOM PGD 12
- MARCORSYSCOM PGD 13 (issue dependent)
- MARCORSYSCOM PGD 14 (issue dependent)
- MARCORSYSCOM PGD 15 (issue dependent)
- MARCORSYSCOM PGD 16 (issue dependent)
- CO, MCTSSA
- Division heads of the C4I/I Support Groups,
- Director, Concepts Branch, Warfighting Requirements Division, MCCDC
- DRPM, AAA
- Support Groups and Teams:

1) Enterprise Interoperability Working Group (EIWG): The EIWG, functioning under the authority of the Director, C4I SE&I Division, is responsible for the oversight and management of Marine Corps C4ISR Service/Joint/Combined interoperability. The EIWG is responsible to the Director C4I SE&I for providing recommendations to facilitate decisions regarding proposed changes to interoperability configuration items, C4I standards, data elements, and Marine Corps positions on Service/Joint/Combined interoperability standards and issues. The EIWG shall also coordinate with IPTs to provide technical oversight for target-related work efforts.

2) Integrated Product Teams: The Target Board, through coordination with all of the MARCORSYSCOM PGDs and other internal/external stakeholders (i.e., independent PMs, HQMC, MCCDC, DRPM AAA, other Services, etc.) shall charter, resource and assign personnel to IPTs as needed to conduct a detailed assessment of targets. These IPTs may have multiple issues under consideration at any one time. Upon completion of these detailed assessments, the IPTs shall present recommended courses of actions to the Target Board addressing programmatic and technical issues as well as identifying resource requirements and a Plan of Action and Milestones (POA&M).

d. Responsibilities:

1) The Commanding General, MARCORSYSCOM, has designated the Deputy Commander, C4I Integration, as the Target Board Chairman. Although all members of the Target Board can provide information and advise through active participation, the Target Board

Chairman is the sole decision maker. The Target Board Chairman is also responsible for ensuring members and working groups adhere to the Target Board process.

2) The Operations Team, C4I/I, MARCORSYSCOM, is responsible for administrative and scheduling support to the Target Board, and is also responsible for the Target Board Secretariat. The Target Board Secretariat performs the administrative functions of the Target Board. The Secretariat resolves all Target Board administration and scheduling issues, as directed by the Target Board Chairman. The Secretariat shall maintain a list of members assigned by each organization to the Target Board. The Secretariat is responsible for the dissemination of all meeting agendas, read-ahead packages, and minutes to all Target Board members. The Secretariat records, and tracks the status and assignment of all Target Board decisions and action items.

3) The Target Board Members identified above shall support the Target Board and provide representatives to Target Board meetings. MARCORSYSCOM PGDs shall also provide staff personnel and other resources as necessary to support IPTs that are chartered by the Target board.

e. Tasks:

1) The Director C4I SE&I Division shall maintain a Marine Corps Enterprise Architecture of integrated operational, systems and technical architectural views. The MCIAP, which documents the Marine Corps Enterprise near-term, C4I systems architecture baseline, shall identify and include information pertaining to the system interfaces that are needed to facilitate systems interoperability across the enterprise-level architecture. The MCIAP baseline shall support the analysis of current and new systems interoperability and integration requirements.

E.3 EIP Target Board Process

a. Receive Target Issues. Issues concerning systems interoperability and integration can come from a number of sources including both internal and external sources to the Marine Corps. The C4I/I Operations Team is responsible for the initial receipt and processing of Target issues, as shown in Figure E-1. Documentation to outline procedures for submitting issues and to describe the Target Process is both posted on the C4I SE&I Knowledge Center and included as an Attachment.

b. Initial Assessment. Upon receipt of an Issue, the Operations Team shall administratively review the Issue for completeness and then forward the Issue to the Systems Engineering Team of C4I SE&I. An initial assessment of the Issue will then be conducted to understand the scope of the problem that is being described and to verify the systems that are impacted, as originally identified by the submitter. To better understand the proposed issue, PGD/PMs may be asked to provide their perspective, as well as Lead System Engineers, other EIWG members, and others as appropriate. Issues that concern systems interoperability and/or integration and meet the following minimum criteria have the potential to become “Targets”:

- Inter-PGD/PM in nature
- Joint interest
- Inter-Service interest
- Marine Corps-wide interest
- Command interest

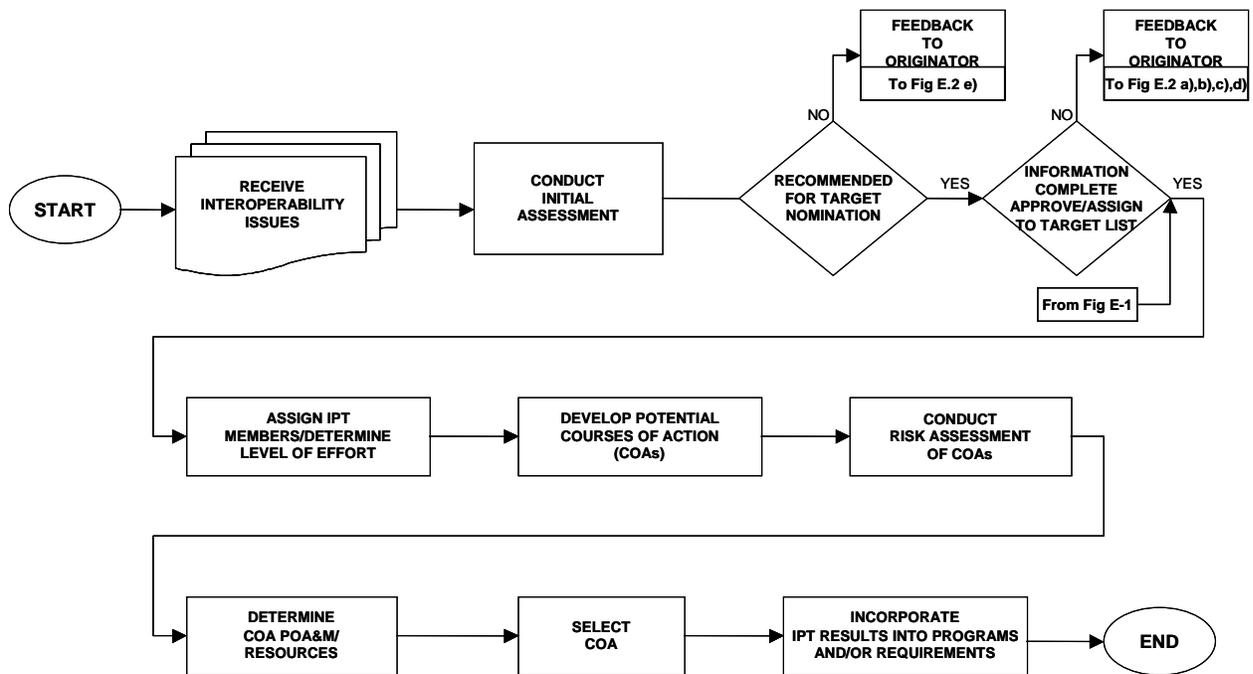


Figure E-1: The EIP Target Board Process

c. Recommendation. Based on the initial assessment, the C4I SE&I Systems Engineering Team will make a determination for further handling of the Issue.

1) Target Nomination. If the Issue meets the criteria outlined above, it can be recommended as a “Potential Target” and submitted to the EIP Target Board for consideration as a qualified “Target”.

2) Feedback to Originator. If the Issue is not recommended as a Target, then C4I SE&I will provide feedback to the Issue originator. The feedback provided can be associated with a number of different cases, each of which requires different follow-up actions on the part of the originator (see Figure E-2):

- a) The Issue needs more information or clarification. The originator provides the additional information or clarification and then re-submits the Issue to C4I SE&I for re-consideration.
- b) The Issue is similar in nature to a Target that is already under consideration. This Issue will be provided to the appropriate IPT.
- c) The Issue falls under the purview of a single PGD/PM; as such, C4I SE&I will forward the Issue to the appropriate PGD/PM.
- d) The Issue pertains to a Joint System for which the Marine Corps does not have primary responsibility; as such, the Issue will be forwarded to the appropriate Agency or Service, and monitored as appropriate. The Issue is given a Target number for monitoring by the Target Board, and may have an IPT assigned to it, but without the responsibility, is not handled as other Marine Corps Target Issues.
- e) The Issue does not meet the criteria of a Target and does not merit action at this time. These issues will be monitored for further developments and may be acted on at a future date.

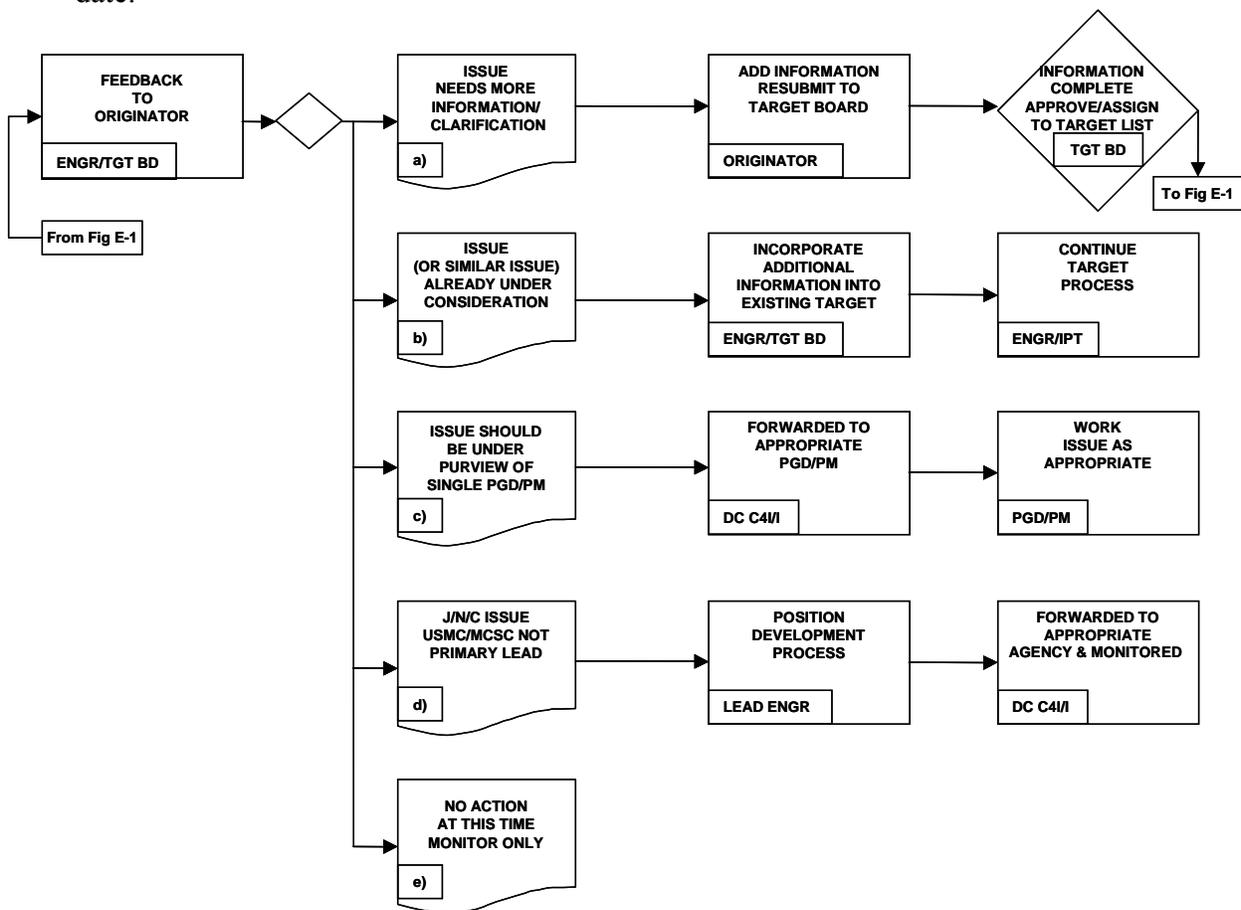


Figure E-2: Feedback to Originator for EIP Target Process

3) Marine Corps “Positions”. There are some issues that will not necessarily lend themselves to being identified as executable interoperability targets, but may require the development of an official Marine Corps position. These technically-oriented issues, which are normally related to Joint, Naval and Coalition matters, will be handled as described below.

- a) Joint Issues. These issues will be assigned to the Enterprise Interoperability Working Group (EIWG) for position development and documentation.
- b) Naval Issues. These issues will be assigned to the C4I SE&I Naval Integration Team for position development and documentation.
- c) Coalition Issues. These issues will be assigned to the appropriate Liaison Officer for position development and documentation.

Once a position has been developed, it will be submitted to the Deputy Commander, C4I/I for approval and dissemination to the appropriate agency (see Figure E-3).

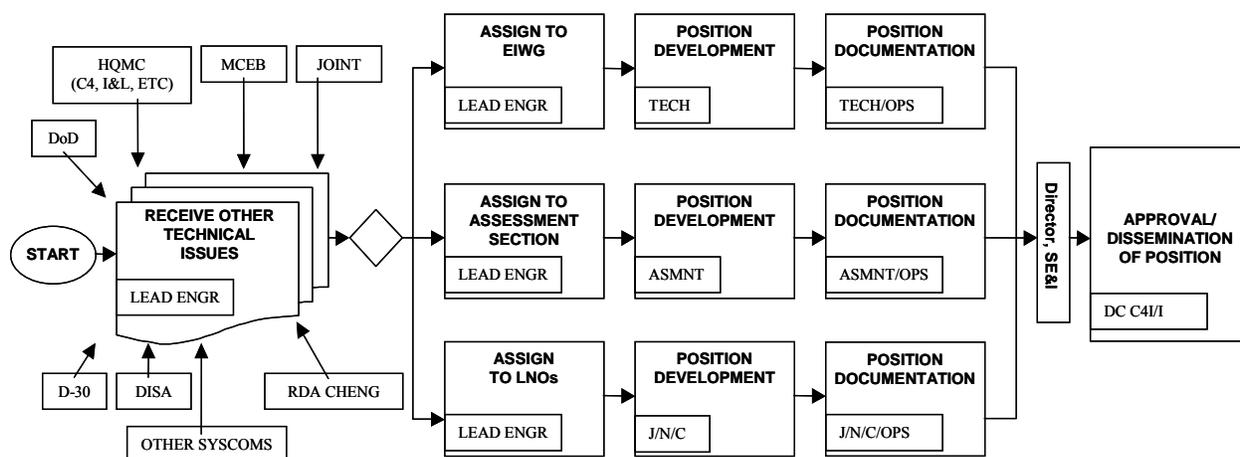


Figure E-3: Development Process for Marine Corps Positions on Joint/Naval/Coalition Issues

d. Approval/Assignment as a Target. The Target Board will review all issues that have been nominated by C4I SE&I as potential Targets. At this decision point, two course of action can result.

1) Approval. If approved, the Target will be added to the Target List and the Target Board will then determine an appropriate level of effort for further investigation. The Target Board will charter an IPT, which will be tasked with conducting an in-depth assessment of the Target.

2) Disapproval. The Target Board will provide feedback to the originator for all “Potential Targets” that are not approved as Targets. This feedback will be provided in the same format and manner as described in paragraph E.3.c.2 above.

E.4 Target Board Integrated Product Teams

An Integrated Product Team (IPT) is a multifunctional team assembled around a product or service, and responsible for advising the Product Leader, Program Manager, or MDA on cost, schedule, and performance of the product. There are three types of IPTs: Overarching IPT, Program IPT, and Working-level IPT (WIPT). The Target Board will use the WIPT.

1) Working-Level IPTs: The Working-level IPT (WIPT) is the type that will be chartered by the Target Board to conduct an in-depth assessment of a selected target(s). The Target Board-sponsored WIPT will be comprised from the Target Board member PGD/Program Manager resources. When necessary, the Target Board may also invite other stakeholders that are not members of the Target Board to provide resources to the WIPT. The WIPT Charter shall

identify the Target to be assessed; the level of effort that should be applied by the WIPT towards assessing the assigned target; and identify all WIPT resources to be used. The WIPT shall be provided access to MCASE and the MCIAP.

2) Target Assessments/Courses of Action (COA): As part of these detailed assessments, the WIPT will develop courses of action (COA) to mitigate or resolve the interoperability and/or integration Target. The WIPT will also conduct a risk assessment, resource requirements and a Plan of Action and Milestones (POA&M) for each COA. The WIPT will then present their assessment to the Target Board with their recommended COAs. The Target Board will select a COA and forward it to the appropriate PGDs/PMs or other stakeholder for incorporation into their programs and/or their project requirements.

E.5 Target Originator's Request:

a. The completed EIP Target Originator's Request (TOR) is an important information component that is used to identify interoperability and integration issues associated with IT systems or NSS affecting the Marine Corps Enterprise Architecture. Essentially, the TOR acts as a "work request" for identifying current and future (systems or technical) interoperability and/or integration issues, and it is the primary means for entry into the Target Process. The TOR identifies systems and/or technical architecture related performance opportunities and deficiencies that impact operational capabilities and overall mission effectiveness. The TOR can also be used to identify potential opportunities, which may include new capabilities, improvements to existing capabilities, and elimination of redundant or unneeded capabilities.

b. Each originator of an issue is required to complete the first part of the TOR. The originator provides information about the primary POC, target type, target description, time frame of potential impact, and the rationale for pursuing this issue as an interoperability and integration issue. The remaining information is for tracking, analysis, and feedback purposes and will be compiled and completed by personnel from the C4I SE&I Division, the Target Board, and/or the assigned WIPT. The entire TOR form is provided in Attachment E-1 and is available on the C4I SE&I Knowledge Center.

THIS PAGE INTENTIONALLY LEFT BLANK

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

PURPOSE

The completed EIP Target Originator's Request (TOR) is an important information component used to identify interoperability and integration issues associated with IT systems or NSS affecting the Marine Corps Enterprise Architecture. Essentially, the TOR acts as a "work request" for identifying current and future (systems or technical) interoperability and/or integration issues, and it is the primary means for entry into the Target Process. The TOR identifies systems and/or technical architecture related performance opportunities and deficiencies that impact operational capabilities and overall mission effectiveness. The TOR can also be used to identify potential opportunities, which may include new capabilities, improvements to existing capabilities, and elimination of redundant or unneeded capabilities.

TOR Routing and Status (For use by C4I SE&I Division)

Reception and forwarding dates for each part of the TOR are summarized here. The numbered processes are identified below in the Target process.

TGT	Actions	Rec'd	Fwd'd
1	Originator Submits Interoperability Issue		
2	C4I SE&I Conducts Initial Assessment		
3a	TGT BD Approves Issue to Target List		
3b	TGT BD Assigns IPT/Determines Level of Effort		
4a	IPT Stands-up - Develops Potential Course of Action		

TGT	Actions	Rec'd	Fwd'd
4b	IPT Conducts Risk Assessments on COAs		
4c	IPT Determines POA&M and Resources for COAs		
5	TGT BD Selects COA - Issues SPD		
6	Results of IPT Incorporated into Program and/or Requirements		

The EIP Target Board Process

(Provided for information and reference)

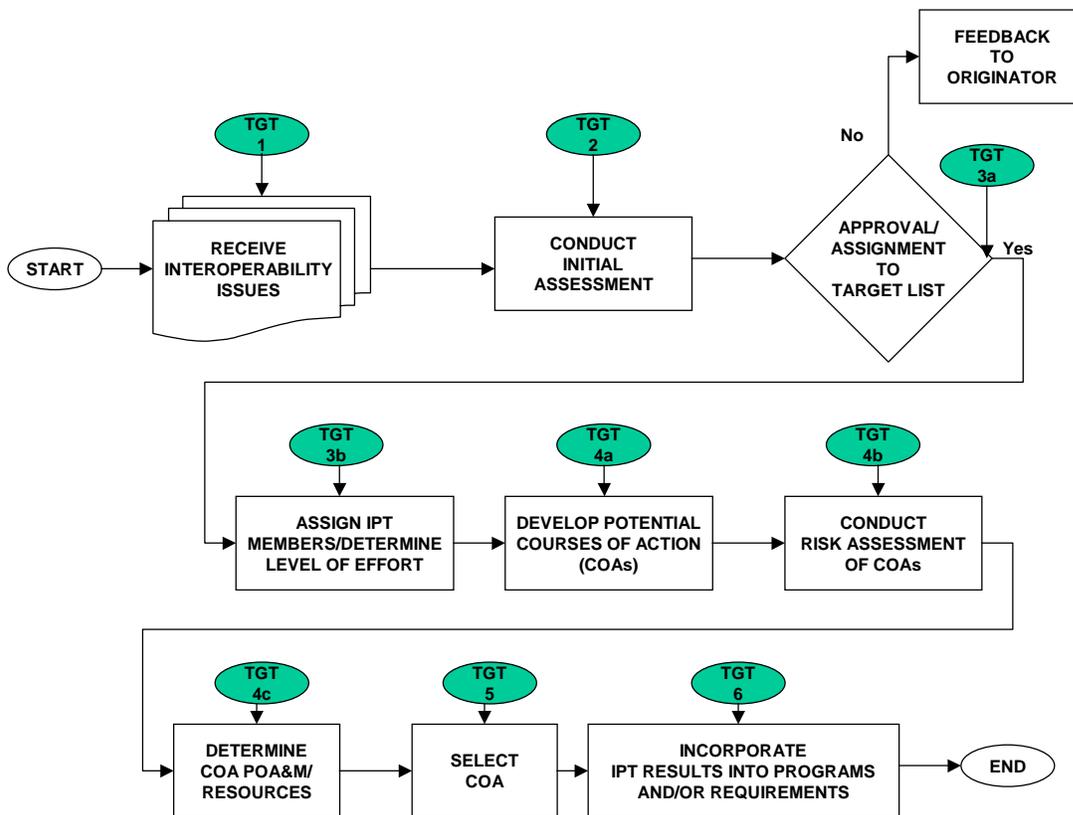


Figure E-1-4: EIP Target Board Process

**C4I Interoperability and Integration Issue
 Target Originator's Request (TOR)
 Part 1 of 6 - Originator**

Target Short Title	For use by MARCORSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Name (Last, First, Initial)	Rank/Grade	Phone	FAX
	Interested in participation on Solution Course of Action IPT?	Request TOR updates by e-mail?	E-mail Address RUC

Target Type (select the appropriate choice – add, improve, or delete capability)

ADD a new capability that does not currently exist		IMPROVE or FIX an existing capability		REMOVE an existing capability	
--	--	---------------------------------------	--	-------------------------------	--

Target Description Describe the nature of the target as it pertains to the condition, consequence, and context.

- a. Condition, Consequence – A complete target description will include a **condition** (a brief statement that describes the circumstances, situation, etc. that outlines the potential threat/opportunity as it relates to the Systems/Technical Architecture. Additionally, the description can include a **consequence** (a short statement that identifies the potential (positive/negative) outcome) of this condition on the Systems/Technical Architecture.
- b. Context - The target statement describes the condition and consequence of target. Additional information should also be collected to provide **context** for the target. This context (what, when, where, how and why) will ensure that the original intent of the target can be understood as it progresses through the entire process.

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Time Frame of Potential Impact to the Marine Corps Integrated Architecture

URGENT		6 Months		1 Year		2 Years		5 Years		10 Years		Other (date)
--------	--	----------	--	--------	--	---------	--	---------	--	----------	--	--------------

Rationale Describe why the target requires resolution in timeframe selected (e.g., interoperability issues, Congressional mandate, etc.).

Performance Impact Describe how the target impacts the performance of the current systems/technical architecture.

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Effectiveness Impact Describe how the target impacts mission or task effectiveness.

Part 2 of 6 – C4I SE&I Systems Engineering Team Review

Action Officer (AO):		AO Email:	
AO Phone:		Date TOR Review Complete:	
Date TOR Forwarded To Target Board:		Date Target Board:	

PGD Involvement

Lead:	
Support:	

TOR Review (Part 1): Describe the Target in the context of its impact to the current Marine Corps Enterprise Architecture.

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

TOR Review (Part 2): Review projects and initiatives currently in the Target Process to determine if the Target is a new initiative, related to current Target initiatives, or redundant (already addressed by the Target Process). When appropriate, the review should include any ongoing Science & Technology initiatives.

Part 3a of 6 - Target Board Endorsement

For use by C4I SE&I

Lead PGD Organization	
POC	Phone
Date Approved	E-mail

**TGT BD
Comments**

Comments shall address TOR Review (Part 1). Modifying comments may address the description of need, the requested timeframe, the mission/task, and benefits and risk. In order to determine the required level of effort, comments shall include any architecture implications, relative prioritization of the target, and dissenting comments from any supporting PGDs.

Target Board Decision to Continue TGT Processing

CONCUR as written. The target is approved for further processing; assign to IPT.

CONCUR as modified by comments. The target, as modified by Target Board comments, is approved for further processing; assign to IPT.

NON-CONCUR. Rationale is provided in Target Board comments. The issue shall be returned to Originator with a copy forwarded to C4I SE&I Assessments Team.

OTHER. Explained in Target Board comments.

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Target Board Comments (Summary):

Part 3b of 6 – Target IPT Assignment

Lead PGD:	
Date IPT Assigned:	
IPT Meeting Date:	
IPT Membership (Lead)	Name/Organization
IPT Membership (Member)	Name/Organization

Target IPT Charter Required level of effort and resources (summary).

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Part 4a of 6 - Target IPT Courses of Action (COA)

Date Entered	COA No.	IPT Summary

Part 4b of 6 - Target IPT Courses of Action (COA) Risk Assessment

Date Entered	COA No.	IPT Summary

Part 4c of 6 - Target Estimate of Supportability

Est. of Supportability Due Date:	
IPT Recommendation:	COA #

Target Estimate of Supportability (POA&M/Resources Summary)

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Part 5 of 6 - Target Board Selects COA

Target Board Selected COA:	COA #	Date of Selection:
SPD Draft Date:	SPD Final Date:	

Description of COA Selected by Target Board

Target Solution Planning Directive (SPD) (Summary)

**C4I Interoperability and Integration Issue
Target Originator's Request (TOR)**

Target Short Title	For use by MARCORSSYSCOM C4I SE&I Division
Target No.	Date Target No. Assigned

Part 6 of 6 - Assignment of IPT Results to Appropriate Program/Requirements

Feedback to Originator

Date of Response to Originator:

Feedback Text

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F: ENTERPRISE INTEROPERABILITY WORKING GROUP CHARTER

Appendix F provides the charters and processes for the Enterprise Interoperability Working Group (EIWG) and associated sub-working groups.

F.1 PURPOSE

This charter establishes the Enterprise Interoperability Working Group (EIWG), which shall function under the authority of the Marine Corps Systems Command (MARCORSYSCOM) C4I Integration Board. Depending on the issues to be addressed, the C4I Integration Board may also function as the Enterprise Integrated Product (EIP) Configuration Control Board (ECCB) or the EIP Target Board.

F.2 RELATIONSHIPS

The EIWG is responsible for providing technical input to the C4I Integration Board and technical oversight of the EIP Target Board Integrated Product Teams (IPTs) as well as Standing Working Groups - the Hardware Working Group (HWG), the Software Working Group (SWWG), the Communications and Network Working Group (C&N WG), and the Cryptographic Modernization Initiative Working Group (CMI WG). The EIWG is also responsible for conducting configuration management of the Marine Corps C4ISR architecture and Joint/Combined C4ISR interoperability standards. The EIWG makes recommendations to the ECCB regarding proposed changes to interoperability configuration items, C4ISR data elements and Marine Corps positions on Joint/Combined C4ISR interoperability standards. Figure F-1 depicts the organizational relationships of the EIWG in accordance with this C4I I&IMP, the C4I EIP Configuration Management Plan (C4I ECMP), reference (f), and the EIP Target Board Charter and Process, Appendix E.

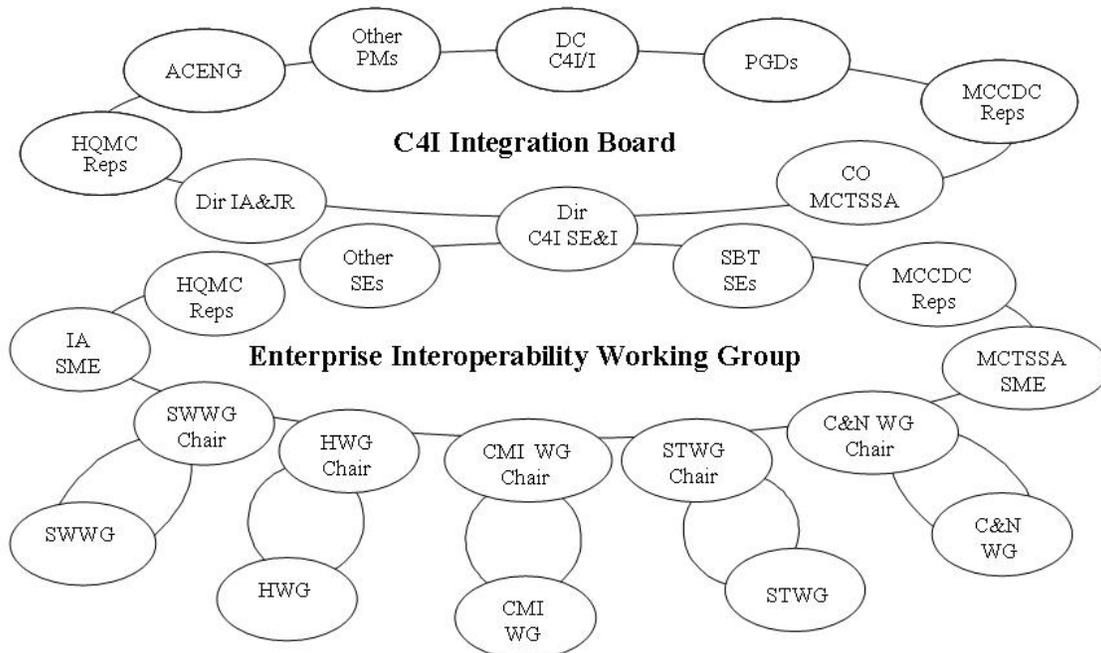


Figure F-1: EIWG Organizational Relationship

F.3 BACKGROUND

The EIWG is central to the Marine Corps interoperability enterprise configuration control process and is the interoperability management hub for development and maintenance of Marine

Corps C4ISR technical architectures and standards. Generally, the EIWG deals with the evaluation and disposition of proposed changes affecting C4ISR systems interfaces, and operational and doctrinal interoperability.

F.4 OBJECTIVE

The objective of the EIWG is to promote interoperability of interfacing C4ISR systems by developing and coordinating workable solutions to interoperability and integration problems.

F.5 MEMBERSHIP

a. The EIWG permanent membership shall consist of the lead systems engineers from the following organizations:

- 1) Chairman: Designated by the Director, C4I Systems Engineering and Integration (C4I SE&I) Division, MARCORSYSCOM
- 2) MARCORSYSCOM Product Group (PG) 10, Information Systems and Infrastructure
- 3) MARCORSYSCOM PG 11, MAGTF C2, Weapons and Sensors Development and Integration
- 4) MARCORSYSCOM PG 12, Communications, Intelligence and Networking Systems
- 5) MARCORSYSCOM PG 13, Infantry Weapons Systems, as required
- 6) MARCORSYSCOM PG 14, Armor & Fire Support Systems, as required
- 7) MARCORSYSCOM PG 15, Ground Transportation and Engineer Systems, as required
- 8) MARCORSYSCOM PG 16, Combat Equipment and Support Systems, as required

Members designated “as required” have full membership status for issues that impact their programs.

b. And representatives from:

- 1) Marine Corps Tactical Systems Support Activity (MCTSSA), SE&I Support Division
- 2) Marine Corps Combat Development Command (MCCDC), Expeditionary Force Development Center, C2 Integration Division
- 3) MCCDC, Expeditionary Force Center, Materiel Requirements Division
- 4) Deputy Commandant for Aviation (DC/A), Headquarter Marine Corps (HQMC)
- 5) Director, Command, Control, Communications, and Computers (C4), HQMC
- 6) Director, Intelligence Department, HQMC
- 7) Direct Report Program Manager, Advanced Amphibious Assault (DRPM AAA)
- 8) MARCORSYSCOM PM Ammunition, as required
- 9) MARCORSYSCOM PM Training Systems, as required
- 10) Marine Corps Warfighting Laboratory (MCWL) Technology Division, as required
- 11) Others as determined by Chairman

c. Supporting IPTs/Working Groups (WGs): The EIWG coordinates with Target Board IPTs and Standing Working Groups.

1) Target Board IPTs under the technical oversight of the EIWG are:

a) Chartered by the Target Board to conduct in-depth assessments of selected targets and systems’ level issues that pose a potential impact to the MARCORSYSCOM Enterprise-Level Systems Architecture.

b) Tasked to conduct detailed assessments of assigned target issues; present recommended courses of action to the Target Board addressing programmatic and technical requirements and a Plan of Action and Milestones (POA&M).

2) Standing Working Groups will propose common material solutions across the Marine Corps Enterprise in their assigned product lines and operate through the EIWG. Standing WGs are established to investigate/address inter-Product Group (PG) issues that respective systems engineers cannot resolve; programs that have an impact of high significance across MARCORSSYSCOM; and programs that involve significant policy issues with agencies outside of the command. Charters for the Hardware, Software, Cryptographic Modernization Initiative, and the Communications and Network Working Groups are provided in Attachments F-1-1 to F-1-4, respectively.

a) Hardware Working Group – Responsible for conducting technical research and developing and presenting recommended courses of action with respect to the Marine Corps Common Hardware Suite (MCHS) computers to acquisition programs.

b) Software Working Group – Responsible for providing technical support and programmatic recommendations to identify and resolve Marine Corps unique requirements and issues with the MAGTF Software Baseline, and other common core software segments. Responsible for coordinating Marine Corps representation and positions in joint software related working groups.

c) Cryptographic Modernization Initiative Working Group – Responsible for providing recommendations for synchronization of fielding and migration to specific cryptographic and key management products that include specific application versions and algorithms.

d) Communications and Network Working Group – Responsible for addressing issues related to the integration of the Joint Tactical Radio Systems into the Marine Corps. This group will also address other Marine Corps communication and network issues that impact interoperability of C4ISR systems.

F.6 TASKS

a. The EIWG shall perform the following tasks:

1) Oversee and manage Target Board IPTs and standing working groups technical activities. Serve as a focal point for Marine Corps participation in joint and combined forums and establish consistent, consolidated Marine Corps positions regarding joint interoperability for applicable C4ISR systems.

2) Propose Marine Corps positions on Joint/Combined C4ISR interoperability policies and provide guidance on development of MARCORSSYSCOM Orders intended to provide interpretation of applicable policies and clarification of roles/responsibilities.

3) Make recommendations to the ECCB regarding proposed Interface Change Proposals (ICPs) and EIP Engineering Change Proposals (EECPs) to interoperability configuration items, C4ISR data elements and Marine Corps positions on joint and combined interoperability standards.

4) Develop guidance for Marine Corps representatives to joint forums (e.g., DOD Information Technology Standards Committee (ITSC), Information Technology Standards Working Groups (ISWGs), Joint Transformation to Tactical Data Enterprise Services (TDES) Integrated Product Team (JT2 ITP), Joint Multi-Tactical Data Link Standards Working Group (JMSWG), Joint Multi-Tactical Data Link Configuration Control Board (JMTCCB), United States Message Text Formatting (USMTF) Technical

Review Panel/Configuration Control Board, Variable Message Format Subgroup (VMFSG), and Combat Net Radio Working Group (CNRWG).

- 5) Identify and forward, to the Target Board, proposed targets, system interoperability and integration issues between systems managed in different MARCORSYSCOM Product Groups that cannot be resolved at lower echelons.
 - 6) Coordinate with Target Board IPTs and provide technical oversight for target related work by conducting peer reviews of IPT results.
 - 7) Establish and organize IPTs, as required, to address specific issues.
- b. The Target Board IPTs will perform the following tasks:
- 1) Conduct a detailed assessment of assigned targets.
 - 2) Present recommended courses of action to the Target Board addressing programmatic and technical issues as well as identifying resource requirements and a POA&M. IPT results shall be coordinated through the EIWG before presentation to the Target Board.
- c. Standing Working Groups will perform the following tasks:
- 1) Create and maintain a charter for their product and processes.
 - 2) Resolve interoperability issues through the Deputy Commander C4I Integration process resulting from routine EIWG review.

F.7 RESPONSIBILITIES

- a. The EIWG Chairman is responsible to the C4I Integration Board, the ECCB, and the Target Board for interoperability and integration issues, and to brief these boards on their relevant actions. The Chairman is responsible for scheduling EIWG meetings, designating meeting locations, and providing reports and briefings to the ECCB and the Target Board. The Chairman shall ensure Target Board IPT technical issues are reviewed by the EIWG and that EIWG recommendations are presented to the Target Board.
- b. The EIWG Secretariat performs the administrative functions of the EIWG. The Secretariat resolves EIWG administrative and scheduling issues as directed by the EIWG Chairman. The Secretariat shall maintain a list of EIWG members as assigned by each organization. The Secretariat is responsible for the dissemination of all meeting agendas, read-ahead packages, and minutes to all EIWG members. The Secretariat records and tracks the status and assignment of all EIWG decisions and action items.
- c. EIWG member organizations shall designate a primary and alternate representative to support the EIWG meetings and ensure their names are provided to the EIWG Secretariat. The Strategic Business Team Lead Engineer shall serve as the Product Group primary EIWG representative.
- d. EIWG members shall be responsible for support of and participation in the EIWG activities as follows:
 - 1) Represent their organization and provide technical support for all EIWG meetings, including subject matter experts to include contractor participation, when required.
 - 2) Provide qualified alternates to work all tasks (including attendance at EIWG and subgroup meetings) when the primary representative is unavailable.
 - 3) Respond to assigned action items in a timely fashion.

e. IPT chairmen are responsible to the EIWG and the Target Board for the status and results of their assigned targets. Each chairman is responsible for scheduling IPT meetings, designating meeting locations, and providing reports and briefings to the EIWG and the Target Board.

f. Standing Working Group chairmen are responsible to the EIWG and the ECCB for the status and results of their assigned tasks. Each chairman is responsible for scheduling WG meetings, designating meeting locations, and providing reports and briefings to the EIWG and the ECCB.

F.8 ADMINISTRATIVE

Meetings. EIWG meetings will be held at the call of the Chairman. Normally meetings will be scheduled quarterly, but high priority interoperability actions may require more frequent meetings. A meeting announcement/agenda will be provided to members prior to each meeting. When required, read-ahead packages will be provided prior to the meeting. Communications with members will be accomplished using e-mail to the maximum extent possible.

a. Decision Making. The working group in open forum shall generate all EIWG recommendations. EIWG decisions will be made by consensus. If there are objections they will be noted in the EIWG minutes and a simple majority vote of the EIWG members shall establish the consensus. The Chairman shall resolve tie votes. If the Chairman is required to cast the deciding vote, the rationale for his vote will be documented in the EIWG meeting minutes. An EIWG member may declare his opposition to a majority vote as substantive during the EIWG meeting. A position paper outlining the majority position and opposing position with supporting documentation will be forwarded, depending on the nature of the issue, to the ECCB or the Target Board for resolution.

b. Action Items. Action items will be assigned at meetings to resolve specific questions at a later date in order to facilitate meeting progress. Once assigned, the Chairman will track action items to closure. The statuses of open action items will be distributed prior to each meeting.

c. Issues. An open issues list will be developed from candidate issues provided by EIWG members and accepted by the Chairman. The status of open issues will be briefed at each meeting. The EIWG will determine which issues are forwarded as targets to the Target Board or as standards issues to the ECCB. The Chairman will assign open issues, not forwarded to the Target Board or the ECCB as action items directed to closure.

d. IPTs/WGs. The EIWG may establish IPTs to address specific issues. The EIWG shall provide technical oversight of Target Board IPTs and Standing Working Groups by reviewing their statuses at each EIWG meeting.

F.9 AUTHORITY

The Enterprise Interoperability Working Group is chartered by the authority of the Deputy Commander, C4I Integration, MARCORSSCOM.

F.10 APPROVAL/ENDORSEMENT

In accordance with signature page.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT F-1: HARDWARE WORKING GROUP CHARTER

F-1.1 PURPOSE. This charter establishes the Hardware Working Group (HWG), which shall report to the Enterprise Interoperability Working Group (EIWG). The Marine Corps Common Hardware Suite (MCHS) Computer HWG shall develop, approve, and maintain the MCHS Allocated Baseline (ABL).

F-1.2 RELATIONSHIPS. The HWG is related to the EIWG, the Marine Corps Systems Command (MARCORSYSCOM) Enterprise Configuration Control Board (ECCB), the Enterprise Integrated Product (EIP) Target Board, and other IPTs and Working Groups (WGs) as depicted in the following diagram. Depending on the issues to be addressed, the C4I Integration Board may also function as the ECCB or the Target Board.

F-1.3 BACKGROUND: The Marine Corps is developing and implementing an information technology (IT) infrastructure, compliant with the Net-Centric Enterprise Services (NCES) to support Marine Corps hardware and software applications' requirements. The Marine Corps established the MCHS program to implement this infrastructure. MCHS provides a limited number of hardware configurations (laptops, workstations, and servers) which operate on Reduced Instruction Set Computer (RISC), or UNIX-based IT platforms, and Complex Instruction Set Computer (CISC), or WINTEL-based IT platforms. It also includes enterprise logistics support of the equipment and affects the actions necessary to purchase computers from standard contract vehicles, such as Blanket Purchasing Agreement (BPA), or Indefinite Delivery Indefinite Quantity (IDIQ). Per MARADMIN 246-00, MCHS does not include peripheral devices (e.g. printers, uninterrupted power supplies).

F-1.4 OBJECTIVES. The HWG will assist in implementing the Marine Corps Information Technology Infrastructure (ITI) to support Marine Corps hardware and software applications' requirements. The HWG shall develop, approve, and maintain the MCHS ABL.

F-1.5 MEMBERSHIP. The MCHS Project Lead (PM NMCI/IT) shall serve as Chairman for the group, and the MCHS support contractor will act as Secretary. Membership shall consist of representatives from the following organizations:

- a. MARCORSYSCOM Chief Information Office (CIO)
- b. Marine Corps Network Operations and Security Command (MCNOSC)
- c. MARCORSYSCOM PG 10: Information Systems and Infrastructure
- d. MARCORSYSCOM PG 11: MAGTF C2, Weapons and Sensors Development and Integration
- e. MARCORSYSCOM PG 12: Communications, Intelligence and Networking Systems
- f. MARCORSYSCOM PG 13: Infantry Weapons Systems
- g. MARCORSYSCOM PG 14: Armor and Fire Support Systems
- h. MARCORSYSCOM PG 15: Ground Transportation and Engineer Systems
- i. MARCORSYSCOM PG 16: Combat Equipment and Support Systems
- j. Direct Report Program Manager, Expeditionary Fighting Vehicle (DRPM EFV)
- k. Command, Control, Communications, and Computers (C4), Headquarters, U.S. Marine Corps (HQMC)
- l. Expeditionary Force Development Center, C2 Integration Division, Marine Corps Combat Development Command (MCCDC)
- m. PM Training Systems (TRASYS)
- n. Marine Corps Tactical Systems Support Activity (MCTSSA)

- o. Marine Forces Atlantic (MARFORLANT)
- p. Marine Forces Pacific (MARFORPAC)
- q. Marine Forces Reserve (MARFORRES)
- r. Marine Forces Europe (MARFOREUR)
- s. Marine Forces South (MARFORSOUTH)
- t. Marine Forces Central Command (MARFORCENT)
- u. Other voting members may be added as requested.

F-1.6 TASKS

- a. The HWG shall develop the MCHS ABL and ensure that:
 - 1) MCHS ABL complies with the ECCB Functional Baseline (FBL);
 - 2) Hardware configuration standards comply with the NCES;
 - 3) Hardware configurations consist of commercial off the shelf (COTS) items and non-developmental items (NDI);
 - 4) Hardware configurations meet requirements of multiple systems, and must be within Authorized Acquisition Objective/Table of Equipment (AAO/TE) allowances;
 - 5) USMC technical and logistical requirements are met.
- b. After the HWG determines that the candidate hardware configurations meet the above criteria, they shall:
 - 1) Comply with ECCB FBL to ensure that the MCHS ABL reflects approved changes;
 - 2) Approve the MCHS ABL;
 - 3) Record and document electronically all changes to the MCHS ABL;
 - 4) Inform PM NMCI/ITI of Products Baseline (PBL) changes.
- c. Review currently selected vendor ‘roadmaps’ for future developments.
- d. Review ongoing and proposed MCHS and HQMC C4 policies and procedures, and make recommendations for improvement as required.
- e. Review the logistics support provided by MCHS and make recommendations for improvement as necessary.

F-1.7 RESPONSIBILITIES

- a. The Chairman shall have the authority and responsibility to lead and direct the MCHS HWG in carrying out its functions. The Chairman will:
 - 1) Schedule and conduct the HWG meetings.
 - 2) Provide reports and briefings to the EIWG and ECCB, as requested.
- b. The members designated in paragraph F-1.5 will report and follow the directions of the HWG Chairman in executing their assigned tasks.

F-1.8 ADMINISTRATIVE

Meetings will be held every four to six months, depending on current issues.

- a. The meetings planned duration and schedule will be an on-going process that will continue at the discretion of the Chairman. The Chairman will notify HWG members via e-mail or Naval Message.
- b. Coordination, discussions, voting, and tasking are accomplished via meetings and Internet technologies i.e., e-mail, video teleconferencing and/or web hosting services.
- c. Voting results will be determined by a majority of those voting. Non-attendees to HWG meetings will be polled electronically. No response to the electronic polling will be registered as a “No Vote”.

d. Individual Project Officers are always invited to attend, but the formal voting responsibility will rest with the Logistics Lead of the Product Group, or their designated representative.

F-1.9 AUTHORITY. The Hardware Working Group is chartered by the authority of the Deputy Commander, C4I Integration, MARCORSYSCOM.

F-1.10.APPROVAL/ENDORSEMENT. Approval of this Charter is tied to approval of the Enterprise Interoperability Working Group Charter, to which this Charter is an attachment.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT F-2: SOFTWARE WORKING GROUP CHARTER

F-2.1 PURPOSE. This charter establishes the Software Working Group (SWWG), which shall report to the Enterprise Interoperability Working Group (EIWG). The Software Working Group shall assist the C4I SE&I Division, Product Group Directors, Direct Report Program Managers, Marine Corps Chief Information Officer (CIO), Marine Corps Combat Development Command (MCCDC), and Marine Corps Systems Command (MARCORSYSCOM) Deputy Commander for C4I Integration with maximizing Software Interoperability and Integration across the Marine Corps Enterprise.

F-2.2 RELATIONSHIPS. The SWWG is related to the EIWG, the Marine Corps Systems Command (MARCORSYSCOM) Enterprise Configuration Control Board (ECCB), the Enterprise Integrated Product (EIP) Target Board, and other IPTs and Working Groups (WGs) as depicted in the following diagram. Depending on the issues to be addressed, the C4I Integration Board may also function as the ECCB or the Target Board.

F-2.3 BACKGROUND. Acquisition of software for IT systems must be accomplished in the larger context of who will use it, how it will be used, and how it will be supported. Various directives and products have been formulated to further the goal of information and data interoperability. While these have assisted in development of interoperable software solutions, the level of discretion inherent in applying standards and guidance has resulted in a less than optimum level of software integration. The C4I I&IMP provides the authority to establish the Software Working Group under the EIWG.

F-2.4 OBJECTIVES. The SWWG will assist in development of a synergistic approach among MARCORSYSCOM product groups (PGs), direct report program managers, and other software development stakeholders to field controlled, secure, integrated and interoperable enterprise-wide Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and supporting software for the Marine Corps. By using common computer hardware, fully integrated software, common data meanings, and approved Joint standards and interfaces with compatible implementations, Marine Corps C4I systems are better positioned, and will have the capability for seamless interoperability regardless of the functional area(s) they support.

F-2.5 MEMBERSHIP. The membership shall consist of representatives from the following organizations:

- a. Chairman: chosen by the Director, C4I SE&I
- b. Systems Engineering and Integration (C4I SE&I) Software Team
- c. Space and Naval Warfare Command (SPAWAR) Liaison to MARCORSYSCOM
- d. Marine Corps Liaison to SPAWAR
- e. MARCORSYSCOM D-30 Coordinator
- f. MARCORSYSCOM C4I/I Information Assurance (IA)
- g. MARCORSYSCOM Chief Information Officer (CIO)
- h. Marine Corps Network Operations and Security Command (MCNOSC)
- i. MARCORSYSCOM PG 10: Information Systems and Infrastructure
- j. Program Manager (PM) Combat Support Information Systems (CSIS) (PMM 101)
- k. PM Navy/Marine Corps Intranet/Information Technology Infrastructure (NMCI/IT) (PMM 102)
- l. PM Enterprise Business and Systems Support (EBSS) (PMM-103)

- m. PM Logistics Information Systems (LIS) (PMM-104)
- n. MARCORSYSCOM PG 11: MAGTF C2, Weapons and Sensors Development and Integration
- o. PM Operation Centers (OC) (PMM 111) BMADS Coordination Team (BCT)
- p. PM Radar Systems (RS) (PMM 112) BCT
- q. PM Air Defense Weapon Systems (ADWS) (PMM 113) BCT
- r. MARCORSYSCOM PG 12: Communications, Intelligence and Networking Systems
- s. PM Ground C2 (PMM 121)
- t. PM Communications (PMM 122)
- u. PM Intel (PMM 123)
- v. MARCORSYSCOM PG13: Infantry Weapons Systems
- w. MARCORSYSCOM PG14: Armor & Fire Support Systems
- x. PM Tanks (PMM 142)
- y. PM Amphibious Assault Vehicle Systems (AAVS) (PMM 143)
- z. MARCORSYSCOM PG15: Ground Transportation & Engineer Systems
- aa. MARCORSYSCOM PG16: Combat Equipment & Support Systems
- bb. PM Test, Measurement and Diagnostic Equipment (TMDE) (PMM 161)
- cc. PM Nuclear, Biological and Chemical (NBC) Defense Systems (PMM 163)
- dd. Direct Report Program Manager, Advanced Amphibious Assault (DRPM AAA)
- ee. Marine Corps Warfighting Laboratory (MCWL)
- ff. Marine Corps Operational Test and Evaluation Activity (MCOTEA)
- gg. Director, Command, Control, Communications, and Computers (C4), Headquarters Marine Corps (HQMC)
- hh. Director, Intelligence Department, HQMC
- ii. Deputy Commandant for Aviation (DC/A), HQMC
- jj. Deputy Commandant for Installations and Logistics, HQMC
- kk. Deputy Commandant for Manpower and Reserve Affairs, HQMC
- ll. MCCDC Requirements
- mm. MCCDC Expeditionary Force Development Center, C2 Integration Division
- nn. Marine Corps Training and Education Command (TECOM)
- oo. Marine Corps Tactical Systems Support Activity (MCTSSA)
- pp. Naval Air Systems Command (NAVAIRSYSCOM) PMA 275 (V-22)
- qq. Naval Air Systems Command (NAVAIRSYSCOM) PMA 276 (H-1)
- rr. Marine Forces Atlantic (MARFORLANT)
- ss. Marine Forces Pacific (MARFORPAC)
- tt. Marine Forces Reserve (MARFORRES)
- uu. Other members may be added as determined by individual issues.

F-2.6 TASKS. The Software Working Group shall:

- a. Provide recommendations for synchronization of fielding and migration to specific software products that include specific application versions and operating systems. This will include:
 - 1) Develop and maintain a list of Marine Corps software packages and operating systems that are candidates for neckdown / convergence.
 - 2) Review the neckdown strategies for software baseline convergence, initially based upon convergence plans of each individual member.

- 3) Develop a Marine Corps transition plan for migration from the COE 3.X baseline to the COE 4.X baseline; and future Joint common services.
- b. Create a master schedule that shows timeframes for use of specific software products by individual systems.
- c. Through the EIWG, identify and make recommendations to the ECCB for configuration management issues at the system-of-systems level.
- d. Draft, refine, and administer the MARCORSYSCOM Software Strategic Plan as necessary.
- e. Act as the technical advisory group to the Marine Corps CIO in determination of the optimum U. S. Marine Corps Software Portfolio.
- f. Create and maintain a listing of technical and programmatic points of contact for Marine Corps tactical data systems programs and support facilities
- g. Provide technical support to HQMC C4 (CIO) for development of the U. S. Marine Corps plan for Data Management and Interoperability (DMI) implementation.
- h. Reconcile Technical Architectures with Operational Architectures/Requirements as related to Software elements.
- i. Gather and distribute technical information supporting interchange with Joint and Service agencies, and act as a conduit for aggregation and promulgation of U. S. Marine Corps input to the DoD Information Technology Standards Registry (DISR), COE, C4ISR Architectural Framework, Global Information Grid (GIG) and other entities as directed.
- j. Assist in reconciliation of elements of the Marine Corps Software Baseline (HQMC list of software) with the MARCORSYSCOM Enterprise Integrated Product systems.
- k. Provide recommendations for update of interoperability instructions as necessary.
- l. Review data strategies and out brief EIWG on list of data strategies/associations across the list.

F-2.7 RESPONSIBILITIES

- a. The Chairman is responsible for validating issues to be presented to the SWWG. The Chairman will:
 - 1) Schedule and conduct the WG meetings.
 - 2) Conduct electronic voting.
 - 3) Disseminate SWWG decisions and recommendations.
 - 4) Provide reports and briefings to the EIWG and ECCB.
- b. The SWWG Secretariat performs the administrative functions of the SWWG. The Secretariat will:
 - 1) Resolve all administration and scheduling issues, as directed by the Chairman. The Secretariat is responsible for the dissemination of all meeting agendas, read-ahead packages, and minutes to all SWWG members.
 - 2) Maintain a list of members of the group, to be maintained as an attachment to this Charter.

3) Record and track the status and assignment of all SWWG decisions, recommendations, and action items. The Secretariat maintains an online compilation of reference documents applicable to SWWG tasks, and administers an electronic voting capability that will reduce the necessity for frequent meetings.

c. The members identified in paragraph F-2.5 shall support the SWWG and provide representatives to SWWG meetings and others as directed.

F-2.8 ADMINISTRATIVE

a. It is anticipated that the SWWG will meet quarterly, with meetings or virtual meetings scheduled as needs dictate.

c. The Secretariat will establish and maintain an electronic decision support presence on the C4I SE&I QuickPlace.

F-2.9 AUTHORITY. The Software Working Group is chartered by the authority of the Deputy Commander, C4I Integration, MARCORSYSCOM.

F-2.10 APPROVAL/ENDORSEMENT. Approval of this Charter is tied to approval of the Enterprise Interoperability Working Group Charter, to which this Charter is an attachment.

ATTACHMENT F-3: COMMUNICATIONS AND NETWORK WORKING GROUP CHARTER

F-3.1 PURPOSE. This charter establishes the Communications and Network Working Group (C&N WG), which shall function under the authority of the Marine Corps Systems Command (MARCORSYSCOM) Enterprise Interoperability Working Group (EIWG) and the Enterprise Integrated Product (EIP) Target Board. The C&N WG is responsible for performing configuration management of the Marine Corps expeditionary communications and network architectures¹. The C&N WG makes recommendations to the EIWG regarding proposed changes to interoperability configuration items, communications/network data elements and Marine Corps positions on Joint/Combined communications and networking interoperability standards. The C&N WG is specifically tasked with addressing issues related to the integration of the Joint Tactical Radio Systems (JTRS) into the Marine Corps expeditionary communications and network architectures.

F-3.2 RELATIONSHIPS. The C&N WG is related to the EIWG, the Marine Corps Systems Command (MARCORSYSCOM) Enterprise Configuration Control Board (ECCB), the Enterprise Integrated Product (EIP) Target Board, and other IPTs and Working Groups (WGs) as depicted in the following diagram. Depending on the issues to be addressed, the C4I Integration Board may also function as the ECCB or the Target Board.

F-3.3 BACKGROUND. The C&N WG is central to the Marine Corps communications and networking configuration control process and is the communications and network interoperability management hub for development and maintenance of Marine Corps communications and networking technical architectures and standards. Generally, the C&N WG deals with the evaluation and disposition of proposed changes affecting communication and network systems interfaces, and operational (doctrinal) and technical interoperability.

F-3.4 OBJECTIVES. The objective of the C&N WG is to promote an integrated communications and network architecture by developing and coordinating workable solutions to interoperability and integration problems.

F-3.5 MEMBERSHIP. The C&N WG membership shall consist of the systems engineers and representatives from the varying organizations.

1. Permanent membership shall consist of the systems engineers from the following organizations:
 - a. Chairman: Designated by Program Manager, Communication Network Systems (CNS), MARCORSYSCOM
 - b. Director, Command, Control, Communications, and Computers (C4), Headquarters Marine Corps (HQMC)
 - c. MARCORSYSCOM System Engineering and Integration; maintains the system and technical Views of the communications architecture
 - d. MCCDC C2 Integration Division; maintains the operational view of the communications architecture.

¹ The Marine Corps' Expeditionary Network is defined in HQMC's C4 Campaign Plan, Second Edition, 2003, "Building the Marine Corps Expeditionary Network (eXNET)" as the expeditionary part of the Marine Corps Enterprise Network (MCEN).

- e. MARCORSYSCOM Product Group (PG) 10, Information Systems and Infrastructure
 - f. MARCORSYSCOM Program Manager (PM) Combat Support Information Systems (CSIS) (PMM 101) - as required
 - g. MARCORSYSCOM PM Navy/Marine Corps Intranet/Information Technology Infrastructure (NMCI/IT) (PMM 102) - as required
 - h. MARCORSYSCOM PG 11, MAGTF C2, Weapons and Sensors Development and Integration - as required
 - i. MARCORSYSCOM PM Operation Centers (OC) (PMM 111) BMADS Coordination Team (BCT) - as required
 - j. MARCORSYSCOM PM Radar Systems (RS) (PMM 112) BCT - as required
 - k. MARCORSYSCOM PM Air Defense Weapon Systems (ADWS) (PMM 113) BCT - as required
 - l. MARCORSYSCOM PG 12, Communications, Intelligence and Networking Systems
 - m. MARCORSYSCOM PM Ground C2 (PMM 121)
 - n. MARCORSYSCOM PM Communication Network Systems (PMM 122)
 - o. MARCORSYSCOM PM Intel (PMM 123)
 - p. MARCORSYSCOM PG 13, Infantry Weapons Systems - as required
 - q. MARCORSYSCOM PG 14, Armor & Fire Support Systems - as required
 - r. MARCORSYSCOM PM Tanks (PMM 142) - as required
 - s. MARCORSYSCOM PM Assault Amphibious Vehicle Systems (AAVS) (PMM 143) - as required
 - t. MARCORSYSCOM PG 15, Ground Transportation and Engineer Systems - as required
 - u. MARCORSYSCOM PG 16, Combat Equipment and Support Systems - as required
 - v. Direct Report Program Manager, Advanced Amphibious Assault (DRPM AAA) - as required
 - w. Marine Corps Warfighting Laboratory (MCWL)
 - x. Marine Corps Operational Test and Evaluation Activity (MCOTEA)
 - y. Director, Intelligence Department, HQMC
 - z. Deputy Commandant for Aviation (DC/A), HQMC
 - aa. Deputy Commandant for Installations and Logistics, HQMC
 - bb. Deputy Commandant for Manpower and Reserve Affairs, HQMC
 - cc. MCCDC Requirements
 - dd. MCCDC Expeditionary Force Development Center, C2 Integration Division
 - ee. Marine Corps Training and Education Command (TECOM)
 - ff. Marine Corps Tactical Systems Support Activity (MCTSSA)
 - gg. Naval Air Systems Command (NAVAIRSYSCOM) PMA 275 (V-22) - as required
 - hh. Naval Air Systems Command (NAVAIRSYSCOM) PMA 276 (H-1) - as required
 - ii. Marine Forces Atlantic (MARFORLANT)
 - jj. Marine Forces Pacific (MARFORPAC)
 - kk. Marine Forces Reserve (MARFORRES)
 - ll. Marine Forces Europe (MARFOREUR)
 - mm. Marine Corps Network Operations and Security Command (MCNOSC)
- Other voting members may be added as determined by individual issues. Members designated “as required” have full membership status for issues that impact their programs.
2. Permanent membership shall also consist of representatives from the following organizations:
- a. Marine Corps Tactical Systems Support Activity (MCTSSA), SE&I Support Division

- b. MARCORSYSCOM PM Ammunition - as required
- c. MARCORSYSCOM PM Training Systems - as required
- d. Others as determined by Chairman

F-3.6 TASKS. The C& N WG shall perform the following tasks:

- a. Oversee and manage the Marine Corps' communication architecture. Serve as a focal point for Marine Corps participation in joint and combined network and communications forums and establish consistent, consolidated Marine Corps communications architecture and its integration to the Global Information Grid (GIG).
- b. Propose Marine Corps positions on DoD communications and networking policies and provide guidance on development of MARCORSYSCOM Orders intended to provide interpretation of applicable policies and clarification of roles/responsibilities.
- c. Identify and forward, to the Target Board, proposed targets, communications and networking issues between systems managed in different MARCORSYSCOM Product Groups that cannot be resolved at lower echelons.
- d. Establish and organize IPTs, as required, to address specific issues.

F-3.7 RESPONSIBILITIES

- a. The C&N WG Chairman is responsible to the EIWG, ECCB and the Target Board for communications and networking issues. The Chairman is responsible for scheduling C&N WG meetings, designating meeting locations, and providing reports and briefings to the EIWG, ECCB, and the Target Board. The Chairman shall ensure Target Board IPT technical issues are reviewed by the C&N WG and that C&N WG recommendations are presented to the EIWG and Target Board.
- b. The C&N WG Secretariat performs the administrative functions of the C&N WG. The Secretariat resolves C&N WG administrative and scheduling issues as directed by the C&N WG Chairman. The Secretariat shall maintain a list of C&N WG members as assigned by each organization. The Secretariat is responsible for the dissemination of all meeting agendas, read-ahead packages, and minutes to all C&N WG members. The Secretariat records and tracks the status and assignment of all C&N WG decisions and action items.
- c. C&N WG member organizations shall designate a primary and alternate representative to support the C&N WG meetings and ensure their names are provided to the C&N WG Secretariat. The Strategic Business Team Lead Engineer shall serve as the Product Group primary C&N WG representative.
- d. C&N WG members shall be responsible for support of and participation in the C&N WG activities as follows:
 - 1) Represent their organization and provide technical support for all C&N WG meetings, including subject matter experts to include contractor participation, when required.
 - 2) Provide qualified alternates to work all tasks (including attendance at C&N WG and subgroup meetings) when the primary representative is unavailable.
 - 3) Respond to assigned action items in a timely fashion.
- e. IPT chairmen are responsible to the C&N WG and the Target Board for the status and results of their assigned targets. Each chairman is responsible for scheduling IPT meetings, designating meeting locations, and providing reports and briefings to the C&N WG, EIWG and the Target Board.

F-3.8 ADMINISTRATIVE

- a. Meetings: will be held as determined by Chairman.
- b. Decision Making. Within the WG, positions are determined and decisions made by achieving consensus through majority vote of the membership. Any member may declare a minority position or their opposition to a position or decision of the WG as substantive. In cases of a substantive issue, it will be documented and forwarded to the EIWG for further consideration and resolution. Decisions made at the WG shall hold unless explicitly reversed by the EIWG.
- c. Action Items. Action items will be assigned at meetings to resolve specific questions at a later date in order to facilitate meeting progress. Once assigned, the Chairman will track action items to closure. The statuses of open action items will be distributed prior to each meeting.
- d. Issues. An open issues list will be developed from candidate issues provided by C& N WG members and accepted by the Chairman. The status of open issues will be briefed at each meeting. The C& N WG will determine which issues are forwarded as targets to the EIWG, Target Board or as standards issues to the ECCB. The Chairman will assign open issues, not forwarded to the EIWG, the Target Board or the ECCB as action items directed to closure.
- e. IPTs/WGs. The C& N WG may establish IPTs to address specific issues. The C& N WG shall provide technical oversight of C& N WG IPTs and Standing Working Groups by reviewing their statuses at each C& N WG meeting.

F-3.9 AUTHORITY. The Communications and Network Working Group is chartered by the authority of the Deputy Commander, C4I Integration, MARCORSYSCOM.

F-3.10 APPROVAL/ENDORSEMENT. Approval of this Charter is tied to approval of the Enterprise Interoperability Working Group Charter, to which this Charter is an attachment.

ATTACHMENT F-4: CRYPTOGRAPHIC MODERNIZATION INITIATIVE WORKING GROUP CHARTER

F-4.1 PURPOSE: The Marine Corps Cryptographic Modernization Initiative Working Group (CMI WG) shall report to the Enterprise Interoperability Working Group (EIWG). The CMI WG shall assist the C4I SE&I Division, Product Group Directors, Direct Report Program Managers, Headquarters Marine Corps C4, Marine Corps Combat Development Command (MCCDC), and Marine Corps Systems Command (MARCORSYSCOM) Deputy Commander for C4I Integration with maximizing Cryptographic and Key Management Interoperability and Integration across the Marine Corps Enterprise. Additionally, the CMI WG will identify programmatic and life-cycle costs not covered under initial procurement to ensure Programs of Record (PORs) are sufficiently planning and budgeting for the DoD mandated upgrades to USMC equipment.

F-4.2 RELATIONSHIPS. The CMI WG is related to the EIWG, the Marine Corps Systems Command (MARCORSYSCOM) Enterprise Configuration Control Board (ECCB), the Enterprise Integrated Product (EIP) Target Board, and other IPTs and Working Groups (WGs) as depicted in the following diagram. Depending on the issues to be addressed, the C4I Integration Board may also function as the ECCB or the Target Board.

F-4.3 BACKGROUND. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) directed a DoD-wide initiative to address the challenges of modernizing DoD cryptographic product inventory and associated key management infrastructure.¹ This direction was based upon compelling evidence regarding the state of the current cryptographic inventory, specifically:

- Based on Security and component technologies that are 20-30+ years old and unless replaced or upgraded will reach the end of its useful cryptographic life.
- Becoming logistically unsupportable in the near future.
- Designed to operate in point-to-point configurations even though DoD is increasingly moving to net-centric information architectures.
- Not designed to support the increased allied, Department of Homeland Security (DHS) and coalition partner interoperability requirements that include the ability to add and delete partners on a very dynamic basis.

Information Assurance (IA) is no longer a luxury but a critical warfighting capability. Within Joint Vision 2020 (JV2020), under the Information Security pillar, DoD established the need to provide the secure, seamless, and collaborative information environment that will enable full situational awareness and information dominance during military operations. To this end, the DoD adopted the Defense-in-Depth approach to IA. The four focus areas of Defense-in-Depth include Local Computing Environments or Enclaves, Enclave Boundaries, Networks, and Supporting Infrastructures. Cryptographic systems are utilized in all four Defense-in-Depth focus areas and support the following security services: Confidentiality, Integrity, Identification & Authentication, and Non-Repudiation. These security services can be used individually or in combination to satisfy the protection requirements of the information.

¹ ASD/C3I memorandum, 23 Feb 01.

NSA has established the Joint Service Cryptographic Modernization Initiative Working Group to manage the Cryptographic Modernization Initiative (CMI). The CMI ensures the availability of logistically supportable cryptographic devices, implementing robust cryptographic algorithms in a cost-effective manner throughout their life cycle. The CMI presents an effective path for DoD to achieve modern security solutions to improve cryptographic robustness and to resolve logistics support issues within the current communications security (COMSEC) inventory. The result will be a modernized cryptographic inventory that enables improved mission capability and enhanced operational effectiveness for our warfighters.

In a related effort, NSA has established the Joint Key Management Infrastructure Working Group to manage the Key Management Infrastructure (KMI). The KMI encompasses all the requirements of the Electronic Key Management System (EKMS) which manages Type I (classified) keys, and the Public Key Infrastructure (PKI) which manages Type III and Type IV (Sensitive But Unclassified) keys. KMI will integrate both these infrastructures into a seamless integrated infrastructure that better supports Joint Vision 2020 and reduces costs to DoD.

F-4.4 OBJECTIVES. The CMI WG will use a synergistic approach among MARCORSYSCOM product groups (PGs), direct report program managers, and other stakeholders to field modernized cryptographic and key-management devices for the Marine Corps in accordance with USMC, DoN, DoD, and National policies to meet CMI and KMI objectives. The CMI WG will assist all stakeholders with identification of C4I I&I requirements related to CMI.

F-4.5 MEMBERSHIP. Within the CMI WG, a member is defined as those listed in this section that are part of a Marine Corps command. Other agencies listed below may act in a liaison capacity only and are not voting members. Representatives to the CMI WG must have at least a SECRET level clearance to participate. When possible the members should have at least one year left in their current assignment upon assignment.

1. Permanent members must have a designated representative at all meetings. The CMI WG chairman must be selected from this group. They shall consist of the following organizations:
 - a. Chairman: chosen by the membership, to serve for one year.
 - b. HQMC C4 (CS)
 - c. HQMC C4 (CP)
 - d. MCCDC Expeditionary Force Development Center, C2 Integration Division
 - e. Deputy Commandant for Manpower and Reserve Affairs, HQMC
 - f. MARCORSYSCOM C4I Systems Engineering and Integration (C4I SE&I)
 - g. MARCORSYSCOM C4I/I Information Assurance (IA)
 - h. MARCORSYSCOM PM Communications (PMM 122)
 - i. Project Officer Public Key Infrastructure/Public Key Encryption (PO PKI/PKE)
2. As Needed Members may participate in voting, and may attend all meetings. They must have a designated representative when requested by the CMI WG chairman. They shall consist of the following organizations:
 - a. MCCDC Requirements Division
 - b. Marine Corps Training and Education Command (TECOM)
 - c. Marine Corps Warfighting Laboratory (MCWL)
 - d. Marine Corps Operational Test and Evaluation Activity (MCOTEA)
 - e. Marine Corps Tactical Systems Support Activity (MCTSSA)

- f. Direct Report Program Manager, Advanced Amphibious Assault (DRPM AAA)
- g. MARCORSYSCOM PG13: Infantry Weapons Systems
- h. MARCORSYSCOM PG14: Armor & Fire Support Systems
- i. MARCORSYSCOM PG 10: Information Systems and Infrastructure
- j. Program Manager (PM) Global Combat Support System-Marine Corps (GCSS-MC) (PMM 101)
- k. PM Navy/Marine Corps Intranet/Information Technology Infrastructure (NMCI/IT) (PMM 102)
- l. PM Enterprise Business and Systems Support
- m. PM Logistics Information Systems
- n. PM Tanks (PMM 142)
- o. PM Assault Amphibious Vehicle Systems (AAVS) (PMM 143)
- p. PM Test, Measurement and Diagnostic Equipment (TMDE) (PMM 161)
- q. PM Nuclear, Biological and Chemical (NBC) Defense Systems (PMM 163)
- r. MARCORSYSCOM PG 11: MAGTF C2, Weapons and Sensors Development and Integration
- s. PM Operation Centers (OC) (PMM 111) BMADS Coordination Team (BCT)
- t. PM Radar Systems (RS) (PMM 112) BCT
- u. PM Air Defense Weapon Systems (ADWS) (PMM 113) BCT
- v. MARCORSYSCOM PG 12: Communications, Intelligence and Networking Systems
- w. PM Ground C2 (PMM 121)
- x. PM Intel (PMM 123)
- y. MARCORSYSCOM Chief Information Officer (CIO)
- z. Marine Corps Network Operations and Security Command (MCNOSC)
- aa. Director, Intelligence Department, HQMC
- bb. Marine Forces Reserve (MARFORRES) MCMO
- cc. Marine Forces Pacific (MARFORPAC) MCMO
- dd. Marine Forces Atlantic (MARFORLANT) MCMO
- ee. First Marine Expeditionary Force (I MEF) MCMO
- ff. Second Marine Expeditionary Force (II MEF) MCMO
- gg. Third Marine Expeditionary Force (III MEF) MCMO

3. Liaison (non-voting) attendees may be invited by the CMI WG chairman when desirable and should be informed of CMI WG decisions.

- a. Director, Cryptographic Modernization (NSA)
- b. Director, Key Management Infrastructure (NSA)
- c. Chief of Naval Operations (CNO N64332)
- d. PEO C4I and Space PMW-161 (Cryptographic Modernization PMO)
- e. Naval Air Systems Command (NAVAIRSYSCOM)
- f. PM Cryptographic Modernization, Army
- g. PM Cryptographic Modernization, Air Force
- h. Marine Corps Liaison to the Director of COMSEC Material System (DCMS)
- i. Marine Corps IA Liaison to the Director, National Security Agency (DIRNSA)

Other members may be added as determined by individual issues.

F-4.6 TASKS. The Cryptographic Modernization Initiative Working Group shall:

- a. Provide recommendations for synchronization of fielding and migration to specific cryptographic and key management products that include specific application versions and algorithms. This will include:
 - 1) Develop and maintain a list of Marine Corps cryptographic devices, software and algorithms that are candidates for convergence to a modernized family of cryptography.
 - 2) Review the convergence strategies for current USMC programs and integrate these into an enterprise baseline.
 - 3) Perform gap analysis on the enterprise baseline in order to:
 - a). Develop a Marine Corps transition plan for modernization of cryptographic devices, algorithms and software in accordance with DoD CMI.
 - b). Develop a Marine Corps transition plan for modernization of key management infrastructure in accordance with DoD CMI.
- b. Create a master schedule that shows timeframes for use of specific cryptographic products and related software versions by individual systems.
- c. Through the EIWG, identify and make recommendations to the ECCB for configuration management issues at the system-of-systems level.
- d. Create and maintain a listing of technical and programmatic points of contact for inter-service cryptographic systems programs and support facilities.
- e. Establish and maintain an electronic collaboration capability through which CMI WG members and associates may solicit and exchange technical and programmatic information.
- f. Provide technical support to HQMC C4 for development of the U. S. Marine Corps Cryptographic Modernization Implementation Plan.
- g. Reconcile Technical Architectures with Operational Architectures/Requirements as related to cryptographic elements.
- h. Identify USMC cryptographic requirement gaps to CG MCCDC, SPAWAR PMW-161, HQMC C4, CNO, and Director NSA (DIRNSA).
- i. Gather and distribute technical information supporting interchange with Joint and Service agencies, and act as a conduit for aggregation and promulgation of U. S. Marine Corps input to the Joint Service Cryptographic Modernization Initiative Working Group, Joint Key Management Infrastructure Working Group, C4ISR Architectural Framework, Global Information Grid (GIG) and other entities as required.
- j. Support COMSEC Cables Program in development of COMSEC requirements for submission to HQMC C4 in accordance with MCO 5239.1.
- k. If additional tasks are required by a majority of the members, they will be presented to the EIWG for approval.

F-4.7 RESPONSIBILITIES.

- a. The Chairman is responsible for validating issues to be presented to the CMI WG. The Chairman will:
 - 1) Schedule and conduct the CMI WG meetings.
 - 2) Conduct electronic voting.
 - 3) Disseminate CMI WG decisions and recommendations.
 - 4) Provide reports and briefings to the EIWG, Joint Service Cryptographic Modernization Working Group (JSCMWG), and Joint Key Management Infrastructure Working Group (JKMIWG).

- b. The CMI WG Secretariat performs the administrative functions of the CMI WG. The Secretariat will:
 - 1) Resolve all administration and scheduling issues, as directed by the Chairman. The Secretariat is responsible for the dissemination of all meeting agendas, read-ahead packages, and minutes to all CMI WG members.
 - 2) Maintain a list of member representatives to the CMI WG.
 - 3) Record and track the status and assignment of all CMI WG decisions, recommendations, and action items. The Secretariat maintains an online compilation of reference documents applicable to CMI WG tasks, and administers an electronic voting capability that will reduce the necessity for frequent meetings.
- c. The members previously identified shall perform action items assigned by the CMI WG chairman, and provide representatives to CMI WG meetings as required by the chairman.

F-4.8 ADMINISTRATIVE

- a. Meetings: Initially meetings will be scheduled every four months. The Chairman may change the frequency to semiannually or quarterly as necessary for the execution of the CMI WG tasks.
- b. Decision Making. Decisions are made by achieving consensus through majority vote of the membership, as defined above. Any member may declare a minority position or their opposition to a position or decision of the CMI WG as substantive. In cases of a substantive issue, it will be documented and forwarded to the EIWG for further consideration and resolution. Decisions made at the CMI WG shall hold unless explicitly reversed by the EIWG.

F-4.9 AUTHORITY. The Cryptographic Modernization Initiative Working Group is chartered by the authority of the Deputy Commander, C4I, Integration, MARCORSYSCOM.

F-4.10 APPROVAL/ENDORSEMENT. Approval of this Charter is tied to approval of the Enterprise Interoperability Working Group Charter, to which this Charter is an attachment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G: ISP DEVELOPMENT PROCESS

G.1 PURPOSE

As described in Section 1, MARCORSYSCOM accomplishes a portion of its CM functions through the use of ISPs. This appendix describes the ISP development and approval process for all Marine Corps-led programs to include all ACAT and non-ACAT programs, including Abbreviated Acquisition Programs (AAPs), and fielded systems, and how they coordinate their effort within MARCORSYSCOM. Attachment G-1 provides details on preparing for the ISP Establishment Review. Attachment G-2 details procedures to follow for ISPs developed for systems outside of the Marine Corps, including procedures to follow when no or inadequate ISPs exist.

G.2 BACKGROUND

The DOD Instruction 4630.8 (reference (h)) and the CJCSI 6212.01 (reference (i)) require the development of ISPs for programs in all acquisition categories when they connect in any way to the communications and information infrastructure. The ISP documents the IT and NSS needs, objectives, interface requirements, and provides a mechanism to identify and resolve C4ISR support shortfalls, and planned solutions at any given phase in a program's acquisition cycle.

G.3 ISP POLICY

The following subsections describe the policy on creation and maintenance of MARCORSYSCOM-generated ISPs.

G.3.1 When Required

ISPs are required for ACAT, non-ACAT, AAPs, and fielded systems that connect in any way to the communications and information infrastructure. The DC C4I/I is the approval authority for this determination, and for all Marine Corps ISPs, regardless of ACAT. ISPs will be used within the command to facilitate interoperability and integration among all C4I systems developed and maintained by all PGDs, programs reporting directly to the Commanding General, and Marine Corps ACAT I and II programs.

G.3.2 ISP Timeframe

When a program meets the criteria specified in reference (i) requiring an ISP, PGDs and PMs will ensure an approved ISP is completed/updated prior to major program reviews or milestone decisions. An ISP is also required in order to submit a system for JITC certification in the absence of a JCIDS document with an NR-KPP, since the ISP provides the approved NR-KPP to which JITC tests. It is DC C4I/I procedure that all fielded systems have a JITC certification before obtaining a renewal of their Authority to Operate (ATO). Refer to reference (j) for further information on JITC certification requirements. The ISP will normally be prepared concurrent with the CDD/CPD, and submitted to the Joint Staff after the CDD/CPD Stage 1 comments have been received and the needed changes to the ISP are incorporated. Table G-1 provides a timetable for submitting ISPs. Due to the timelines for USMC and Joint staffing of the ISP, it is recommended that a draft ISP be provided to IA&JR Division four months prior to the milestone or fielding date. If the system requires a JITC certification (e.g., subsequent ATO), it is recommended that a draft ISP be provided to IA&JR Division six months prior to the milestone or fielding date.

G.3.3 ISP Maintenance

Once completed, an ISP shall be kept current through its entire lifecycle, and updated if undergoing a major upgrade, product improvement, or 3-year JITC recertification. Approved

ISPs will be used to monitor the progress of the system toward meeting its interoperability and integration goals.

ISP Type	Initial	Revised	Final	Revised (Upgrade)
ACAT I and Special Interest (SI)	MS B/ PDR	MS C/ CDR	IOC/ FRP DR	Major System Increments
	Developed by PM, reviewed by DC C4I/I and submitted to ASD(NII)/DoD CIO via JCPAT-E. 3-stage Joint-level review.	Same as Initial	Final ISP of record approved and signed by the Component and provided to ASD(NII)/DoD CIO via JCPAT-E. No Joint-level review of the final plan.	Process repeated for each major acquisition increment (upgrade).
ACAT II, III, IV	Developed by PM, reviewed by DC C4I/I and submitted to J6 via JCPAT-E. J6 reviews for correct format and completeness.	Same as Initial	Final ISP of record approved and signed by the Component and provided to ASD(NII)/DoD CIO via JCPAT-E. J6 reviews for correct format and completeness.	Process repeated for each major acquisition increment (upgrade).
Non-ACAT (Including AAP and procurements resulting from an Urgent UNS)	Required for system fielding. Developed by PM, approved by DC C4I/I, posted to JCPAT-E. J6 reviews for correct format and completeness. The process for rapid acquisition (Urgent Universal Need Statements (UNS)) systems will be published separately based on clarification from the Joint staff.			
Fielded System	If managed as an acquisition program, i.e., an increment or spiral, per DoD 5000 series guidance, will be staffed and certified IAW the procedures for ACAT ISPs as described above.			
	All other fielded system ISPs, e.g., for 3 year JITC testing and recertification, or subsequent ATO, will be developed by PM, approved by DC C4I/I, posted to JCPAT-E. J6 reviews for correct format and completeness.			

Table G-1: ISP Submission Timetable and Required Joint Reviews.

G.4 PROCEDURES

Figure G-1 provides a diagram of the process for the preparation and approval of ISPs. The figure is labeled with numbers to correspond to the procedures outlined below, e.g., “Plan accepted? 8” relates to step 8 in paragraph G.4.8.

G.4.1 Step 1. IA&JR Reviews Program for ISP Requirement

IA&JR Division assists the PM by screening all programs listed in CAPS, MCASE, and the Marine Corps Application Portfolio (MCAP) for ISP applicability. The IA&JR Division will

coordinate with Program Managers (PMs) in developing a recommendation as to whether or not an ISP is required. The results of the screening are maintained in the CSAR within MCASE. MCASE is reconciled with CAPS on a regular basis. If a program's information is maintained in CAPS, it will be updated through automated replication in MCASE. New programs should contact IA&JR to have ISP requirements determined. One of two determinations will be made during the screening process:

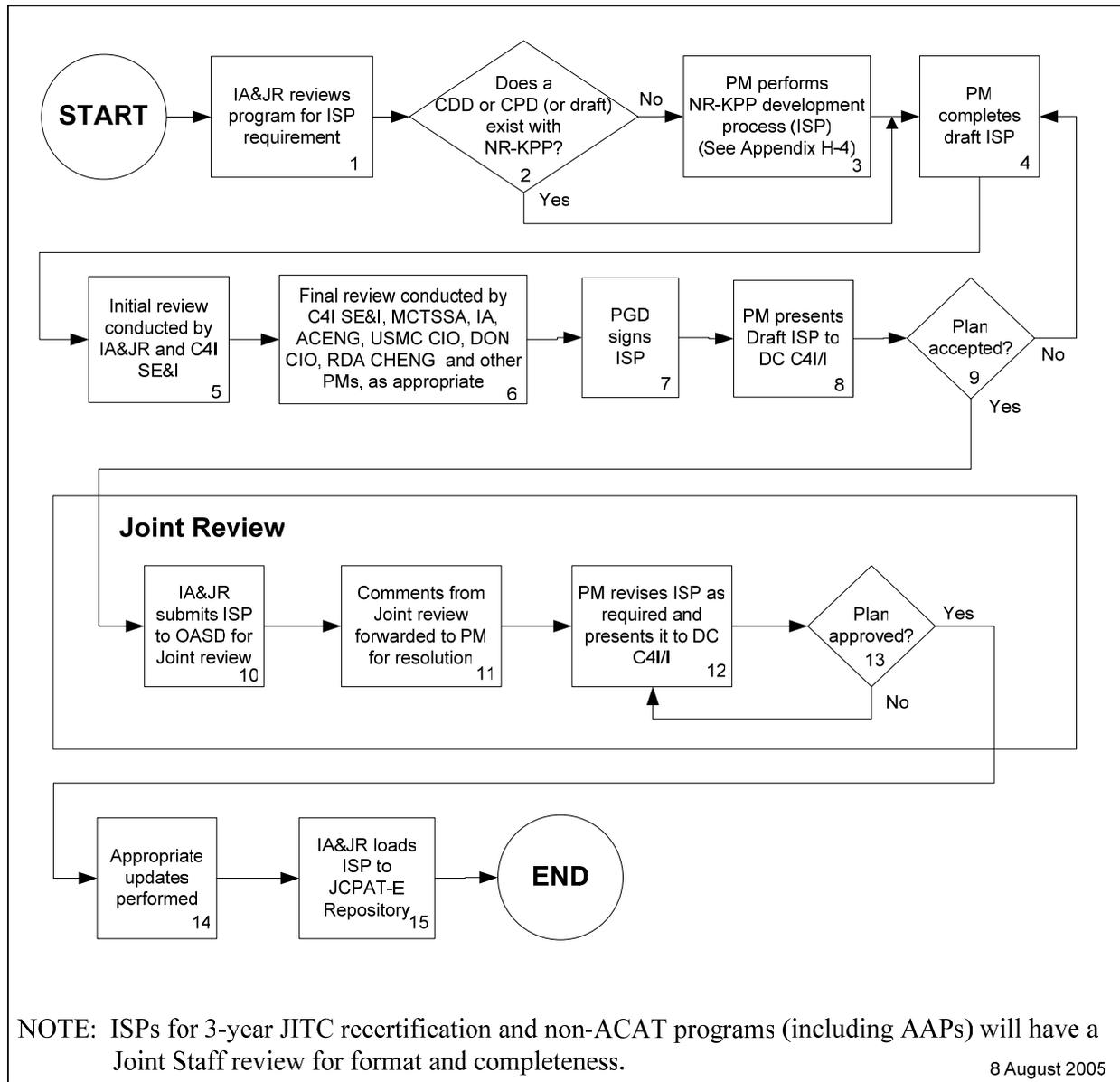


Figure G-1: ISP Preparation and Approval Process

a. **No ISP is required.** The program does not have a reasonable impact, interface, or connection to any system within the Marine Corps communications and information infrastructure. The program will be issued a determination notification from IA&JR indicating that either no action is required or that the PM needs to provide the minimal set of architecture views (SV-2, SV-6, SV-8 and TV-1) in which case a modified version of the process is done. This modified process is described in Section G.5.

b. **An ISP is required.** The program will be issued a written determination from DC C4I/I indicating that an ISP is required based on its potential impact to the Marine Corps communications and information infrastructure. Continue the process in Step 2.

G.4.2 Step 2. Does a CDD or CPD (or draft) exist containing an NR-KPP?

G.4.3 Step 3. No, CDD/CPD (or draft) containing NR-KPP does not exist – PM performs NR-KPP Development Process (ISP).

If no CDD or CPD currently exists (or is in draft) that contains an NR-KPP, the PM will complete an NR-KPP, described in Appendix H (NR-KPP Development Process (ISP)), and return to continue the ISP Preparation and Approval Process using the ISP template (ISP Template with NR-KPP). The ISP template, located in the C4I/I Knowledge Center, provides the easiest means to complete a draft ISP that meets the mandated ISP requirements.

G.4.4 Step 4. Yes, CDD/CPD containing NR-KPP (or draft) does exist. -- PM Completes Draft ISP.

If a CDD/CPD (or draft) exists, the PM shall prepare the remaining portions of the ISP using the ISP template (ISP Template without NR-KPP). The ISP template, located in the C4I/I Knowledge Center, provides the easiest means to complete a draft ISP that meets the mandated ISP requirements. PMs shall adjust their acquisition strategy as necessary to implement the standards and connectivity depicted in the architectural views.

G.4.5 Step 5. Initial Review Conducted by IA&JR and C4I SE&I Divisions

After the draft ISP is completed, it is submitted by the PM to IA&JR Division for initial review. During the initial review process, IA&JR and C4I SE&I Divisions will work with PMs to clarify ambiguities and resolve interoperability and integration issues.

- a. The ISP is reviewed by the IA&JR ISP Team and the C4I SE&I Architecture Team for accuracy of the architectural products and the required elements of the ISP.
- b. The initial TVs are developed by IA&JR and delivered to the PO. The TVs are finalized by the PO and IA&JR once the SV-2 and SV-6 are completed.
- c. During this time, IA&JR will register the program into the Joint C4I Program Assessment Tool – Empowered (JCPAT-E) repository, if required, and upload and publish the Technical Standards Profile (TV-1) on the SIPRnet DISRonline website. (Refer to the JCPAT-E Tutorial on the C4I/I ISP Training Disk located on MCASE for more information).
- d. PM will make corrections as necessary, and have re-reviewed in Step 5a, until all corrections have been made.

G.4.6 Step 6. Final Review Conducted by C4I SE&I, MCTSSA, IA, ACENG, USMC CIO, DON CIO, RDA CHENG and other PMs, as appropriate

After a final draft ISP is completed, it is submitted by the PM to IA&JR for review. During the final review process, the IA&JR and C4I SE&I Divisions will work with PMs to clarify ambiguities and resolve interoperability and integration issues.

- a. IA&JR will staff the ISP to be reviewed by C4I SE&I Division, Marine Corps Tactical Systems Support Activity (MCTSSA), Information Assurance (IA) Teams, Assistant Commander Engineering (ACENG), the USMC CIO, DON CIO, RDA CHENG and the PMs of connected systems that are outside the PG. The PMs are responsible for providing to IA&JR the points of contact information of the PMs of interfacing systems or copies of approved Memorandums of Agreement (MOA), Interface Requirements Specification, or

Interface Design Documentation the system's program office has with the interfacing systems.

b. After final corrections are made to the ISP, the PM and the Director IA&JR shall sign the ISP.

G.4.7 Step 7. PGD Signs ISP

The Product Group Director signs the ISP signifying concurrence.

G.4.8 Step 8. PM Presents Draft ISP to DC C4I/I

In this step of the ISP process, the PM coordinates with IA&JR to set up the ISP Establishment Review, and the PM is responsible for conducting the review with the DC C4I/I. The PM, Project Officer (PO), PGD Lead Engineer, and representatives from the C4I SE&I Division, MCTSSA and IA&JR Division attend the ISP Establishment Review. IA&JR will also coordinate the attendance at the review with PMs of connected systems that are outside the PG and whose connection is not documented by interface control documentation or a memorandum of agreement that is referenced in the ISP. Refer to Attachment G-1 and the C4I/I ISP training disk located on MCASE for more details on preparing for the ISP Establishment Review. For systems with a limited number of interfaces, the ISP Establishment Review briefing may be done via a "paper" process at the discretion of DC C4I/I. This "paper" process would still require development of the briefing slides for review, but would not require a formal briefing from the PM.

G.4.9 Step 9. Plan Accepted?

Depending on the outcome of the ISP Establishment Review, DC C4I/I will either accept the ISP for Joint staffing or return it to the PM/PGD for modification.

a. If accepted, the DC C4I/I will accept the ISP for Joint staffing.

b. If returned, the ISP will be modified, and reenter the approval process in Step 4.

G.4.10 Step 10. IA&JR Submits ISP to OASD for Joint review

After the DC C4I/I has accepted an ISP at Step 9, the DIR IA&JR will electronically submit the document to the Office of the Assistant Secretary of Defense (OASD) via JCPAT-E for Joint review. ISPs for 3-year JITC recertification and ISPs for non-ACAT programs, including AAPs, will be reviewed by the Joint Staff for format and completeness. See Table G-1. The Joint review, as coordinated through OASD, will take 30 days to complete.

G.4.11 Step 11. Comments from the Joint review forwarded to PM for resolution

OASD (for ACAT I/SI) and J-6 (for all others) will consolidate all comments received on the ISP, and return them to the PM (via IA&JR through JCPAT-E) for resolution.

G.4.12 Step 12. PM revises ISP as required and presents it to DC C4I/I

When the comments to the ISP are received, the PM resolves the issues addressed, and revises the document as needed. The PM works with each reviewer to adjudicate the comments, and provides the reviewed comments, with the PM adjudication included, and an updated ISP if required, to IA&JR via both NIPRnet and SIPRnet. The results are to be briefed to the DC C4I/I by the PM. Per the CJCSI 6212.01, the PM will use the issues developed in the ISP process to influence the design review. If an issue cannot be resolved by the PM due to scope or subject matter, the DIR IA&JR, or DC C4I/I may be brought into the resolution process for assistance. After the ISP has been revised, it is presented once again to the DC C4I/I along with an adjudicated comments resolution matrix for final approval and signature.

G.4.13 Step 13. Plan Approved?

- a. No – If the plan is not approved, the ISP will be modified, and reenter the approval process in Step 12
- b. If the plan is approved, the DC C4I/I will sign the ISP.

G.4.14 Step 14. Appropriate Updates Performed

- a. The DIR IA&JR updates the CSAR in MCASE and the DIR C4I SE&I updates the Marine Corps Integrated Architecture Picture (MCIAP).
- b. For programs where the Commanding General is the MDA, the PM/PGD submits a copy of the signed document to the Assistant Commander, Programs, for inclusion in preparatory documentation for the next scheduled milestone decision.

G.4.15 Step 15. Load ISP to JCPAT-E

The DIR IA&JR shall be responsible for posting of the final document and adjudicated comments to the JCPAT-E repository.

G.5 THE PROCESS FOR HANDLING 2681s

The IA&JR review of a program for an ISP requirement, in Step 1, paragraph G.4.1, may conclude that a full ISP is not required, but that a minimal set of architecture views will suffice at this time. Examples where an ISP may not be required and a 2681 is required is for an already fielded system not being upgraded and not needing JITC certification or an ATO. Another example would be for a system used but not developed by the Marine Corps, and the developing Service does not have an appropriate ISP showing Marine Corps interfaces. If the system falls into this category where it meets the criteria for inclusion in the EIP, but does not require an ISP at this time, the program will be issued a determination notification from IA&JR to direct the PM to provide the minimal set of architecture views (SV-2, SV-6, SV-8 and TV-1). Once the 2681 is approved, this minimum set stands in lieu of the ISP for the program until its next system upgrade and creation of a full ISP, including an NR-KPP. The abbreviated ISP process for handling 2681s is as follows:

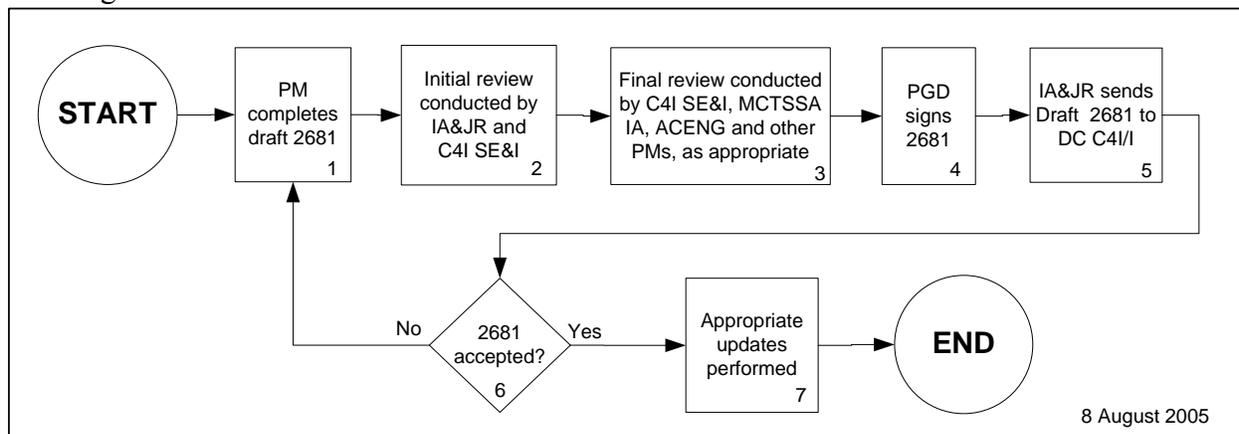


Figure G-2: 2681 Preparation and Approval Process

G.5.1 Step 1. PM Completes draft 2681

PM shall prepare a draft 2681 using the 2681 template. The 2681 template, located in the C4I/I knowledge center, provides the easiest means to complete a draft 2681 that meets the mandated requirements. PMs shall adjust their acquisition strategy as necessary to implement the standards

and connectivity depicted in the architectural views. IA&JR and C4I SE&I Divisions will support the PMs in developing the SV-2, SV-6 and SV-8.

G.5.2 Step 2. Initial Review Conducted by IA&JR and C4I SE&I Divisions

After the draft 2681 is completed, it is submitted by the PM to IA&JR Division for initial review. During the initial review process, IA&JR and C4I SE&I Divisions will work with PMs to clarify ambiguities and resolve interoperability and integration issues.

- a. The ISP is reviewed by the IA&JR ISP Team and the C4I SE&I Architecture Team for accuracy of the architectural products and the required elements of the 2681.
- b. The TV-1 is developed by IA&JR and delivered to the PO once the SV-2 and SV-6 are completed. The TV-1 is finalized by the PO and IA&JR.
- c. PM will make corrections as necessary, and have re-reviewed in Step 5a, until all corrections have been made.

G.5.3 Step 3. Final Review Conducted by C4I SE&I, MCTSSA, IA, ACENG, and other PMs, as appropriate

After a final draft 2681 is completed, it is submitted by the PM to IA&JR for review. During the final review process, the IA&JR and C4I SE&I Divisions will work with PMs to clarify ambiguities and resolve interoperability and integration issues.

- a. IA&JR will staff the 2681 to be reviewed by C4I SE&I Division, Marine Corps Tactical Systems Support Activity (MCTSSA), Information Assurance (IA) Teams, Assistant Commander Engineering (ACENG), and the PMs of connected systems that are outside the PG. The PMs are responsible for providing to IA&JR the points of contact information of the PMs of interfacing systems or copies of approved Memorandums of Agreement (MOA), Interface Requirements Specification, or Interface Design Documentation the system's program office has with the interfacing systems.
- b. After final corrections are made to the 2681, the PM and the Director IA&JR shall sign the ISP.

G.5.4 Step 4. PGD Signs 2681

The Product Group Director signs the 2681 signifying concurrence, and IA&JR schedules the ISP Establishment Review with the DC C4I/I.

G.5.5 Step 5. IA&JR sends Draft 2681 to DC C4I/I.

IA&JR will forward the 2681 to DC C4I/I for approval.

G.5.6 Step 6. 2681 accepted?

- a. No – If the plan is not approved, the 2681 will be modified, and reenter the approval process in Step 1
- b. If the plan is approved, the DC C4I/I will sign the ISP.

G.5.7 Step 7. Appropriate Updates performed

IA&JR uploads the 2681 to the CSAR in MCASE, and C4I SE&I updates the MCIAP.

G.6 RESPONSIBILITIES

The specific responsibilities of the various groups and individuals involved in the ISP process are provided in Section 6, Roles and Responsibilities.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT G-1: ISP ESTABLISHMENT REVIEW PROCESS

G-1.1 Purpose

ISPs will be used within the command to facilitate interoperability and integration among all C4I systems developed and maintained by all PGDs, programs reporting directly to the Commanding General MARCORSSYSCOM, and Marine Corps ACAT I and II programs. ISPs are required at Milestones B, C and all subsequent major modifications to the system, and for the initial JITC certification and the 3-year JITC recertification. The Deputy Commander C4I Integration (DC C4I/I) is the Marine Corps approval authority for all ISPs. This Attachment provides additional information on the formal ISP Establishment Review process used to present ISPs to the DC C4I/I for approval.

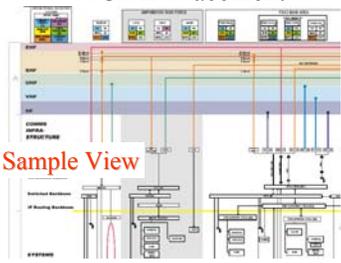
G-1.2 Background

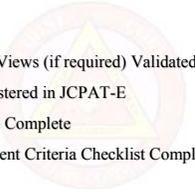
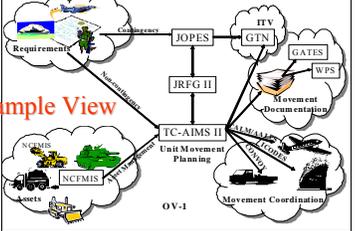
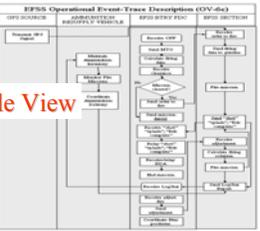
Program Managers and IA&JR Division will work together to make a determination on whether an ISP will be required for each program listed in the EIP, which takes inputs from CAPS, MCASE and MCAP. The program office will be notified directly if an ISP is required. It is critical to ensure that the Next Milestone Date is kept current in CAPS. When an ISP is required, adequate preparation time should be planned to allow for the ISP Establishment Review to be completed at least 90 days prior to the next milestone event.

G-1.3 Procedures

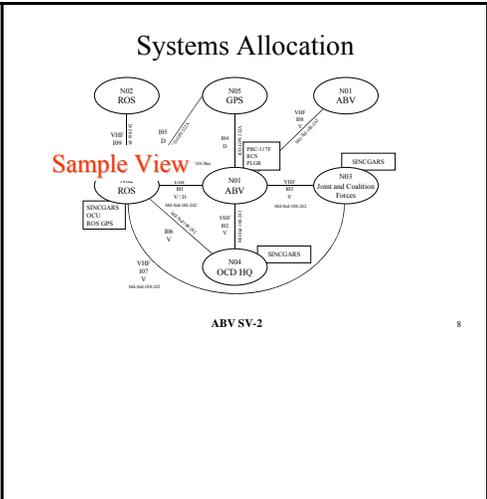
- a. Tab 1 provides a briefing template to prepare for the ISP Establishment Review. The template is also available on MCASE. The CM and ISP Team in IA&JR Division will provide assistance to PMs preparing for the ISP Establishment Review briefings. Scheduling the briefing will be the responsibility of the IA&JR, but coordinated with the PM.
- b. For systems with a limited number of interfaces, the ISP Establishment Review briefing may be done via a “paper” process at the discretion of DC C4I/I. This “paper” process would still require development of the briefing slides for review, but would not require a formal briefing from the PM.

TAB 1 to ATTACHMENT G-1: ISP Establishment Review Template

<p>Slide 1</p>	<p style="text-align: center;">Program XXX ISP Establishment Review</p>  <p style="text-align: center;">Date _____</p> <p style="text-align: right;">Program Manager: _____</p> <p style="text-align: right;">1</p>	
<p>Slide 2</p>	<p style="text-align: center;">Agenda</p> <ul style="list-style-type: none"> • Overview (Prog Desc and MCIAP Placement) • Compliance • Mission and Requirement Analysis (OV-1) • Functional Flow Analysis (OV-2, OV-6C) • System Views (SV-2, SV-5, SV-6, SV-8) • Standards (TV-1) • Net Centric Analysis • Testing • Issues and Risks • Summary <p style="text-align: right;">2</p>	<p>The format for the ISP Establishment Review was built on the general outline provided for a System Requirements Review (SRR) as detailed in MIL-STD 1521B (Appendix B). The information provided in the brief is based on details from the ISP.</p>
<p>Slide 3</p>	<p style="text-align: center;">Program Description</p> <p>The USMC HIMARS will provide ground-based, responsive General Support/General Support-Reinforcing (GS/GSR) indirect fires which accurately engage targets at long range with high volumes of lethal fire under all weather conditions throughout all phases of combat operations ashore.</p> <p>The USMC HIMARS Program is integrating, not developing, Principal End Items (PEIs) and munitions. The USMC HIMARS Program involves the Horizontal Technology Integration (HTI) of three PEIs; the Launcher, the Re-Supply Trailer (RST), and the Re-Supply Trailer (RST). The USMC HIMARS also includes a basic load of production munitions. The US Army is developing the Launcher, and the USMC MTRV Program Office is developing the RSV and RST. The basic load will be selected from the Multiple Launch Rocket System (MLRS) Family of Munitions (MFOM) developed by the US Army and in production.</p> <p style="text-align: right;">3</p>	<p>A Program Description provides an overall synopsis of the system being acquired. The description from CAPS is usually sufficient</p>
<p>Slide 4</p>	<p style="text-align: center;">MCIAP Placement</p>  <p style="text-align: center;">Sample View</p> <p style="text-align: right;">4</p>	<p>The graphic used for the slide should be taken from the MCIAP (“Big Picture”) available on the MCASE web site in the architecture section.</p> <p>In the brief: Indicate where the system being acquired fits into the MCIAP.</p>

<p>Slide 5</p>	<p style="text-align: center;">Compliance</p>  <ul style="list-style-type: none"> ✓Operational Views (if required) Validated by MCCDC ✓System Registered in JCPAT-E ✓DISR Profile Complete ✓ISP Assessment Criteria Checklist Complete <p style="text-align: right;">16</p>	<p>The Compliance slide addresses compliance issues for the ISP.</p> <p>In the brief: Be prepared to address if any of these items have not been completed.</p> <p>The OV's, once completed, shall be submitted to MCCDC (program sponsor or OA Division) for validation, and also to the Functional Sponsor for AISs. This validation may be accomplished via email. A copy of the email shall be provided by the PM at the ISP Establishment Review.</p>
<p>Slide 6</p>	<p style="text-align: center;">High Level Mission and Requirement Analysis</p>  <p style="text-align: center;">Navy Implementation of TC-AIMS II OV-1</p> <p style="text-align: right;">5</p>	<p>The High-level Operational Concept Graphic (OV-1) provides a pictorial of the missions, high-level operations, organizations, and geographical distribution of assets. Its main utility is as a facilitator of human communication, and it is intended for presentation to high-level decision makers. The lines connecting the icons can be used to show simple connectivity, or can be annotated to show what information is exchanged.</p> <p>In the brief: Address where the system being acquired fits into the bigger architecture picture. When possible, reference the capabilities document that is driving the acquisition of the system.</p>
<p>Slide 7</p>	<p style="text-align: center;">Functional Flow Analysis</p>  <p style="text-align: center;">EFSS – OV-2</p> <p style="text-align: right;">6</p>	<p>The Functional Flow Analysis is best depicted by the Operational Node Connectivity Description (OV-2) and Operational Event – Trace Description (OV-6C) slides from the ISP. The OV-2 provides a pictorial of the information exchanges and the OV-6C provides operational activity sequence and timing. Use separate slides to present the OV-2 and OV-6C.</p> <p>In the brief: Talk to the major (or significant) information exchanges that occur at, or through, the node where the system being acquired is located. (This isn't the time to talk to the "systems" being acquired; emphasize the business or operational aspect of the information exchanges.) Identify which information exchanges are CDD/CPD/ORD based. Identify which information exchanges are not CDD/CPD/ORD based.</p>
<p>Slide 8</p>	<p style="text-align: center;">Functional Flow Analysis (Continued)</p>  <p style="text-align: center;">OV-6C Example from EFSS Information</p> <p style="text-align: right;">7</p>	

Slide 9

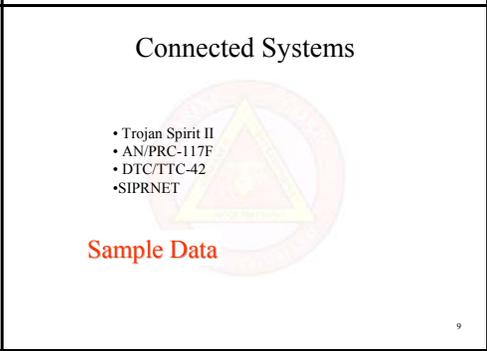


The Systems Allocation paints a picture of what systems are used to fulfill the connectivity to the system being acquired. The view from the ISP providing the information needed for the brief is the Systems Communications Description (SV-2). The SV-2 is an expansion of the SV-1, and depicts the specific network and communication pathways for the systems indicated in the SV-1 graphic.

In the brief:

- Emphasize what systems are connected to the system being acquired.
- Be prepared to address needed changes in AAOs for the systems that connect to the system being acquired, and whether those program offices are aware of the changes.
- Be prepared to talk to whether the system being acquired is using, or planning to use the Marine Corps Common Hardware Suite.
- Be prepared to identify the connectivity that are CDD/CPD/ORD based, or non-CDD/CPD/ORD based.

Slide 10



The Connected Systems should address the cost and operational advantages for selecting the systems that provide connectivity to the system being acquired.

In the brief:

- Emphasize the advantages/reasoning for selecting the systems that are connected to the system being acquired.
- Be prepared to address what systems were not chosen, and the reasoning behind that decision.
- If necessary, note the selection of the systems as related to the requirements provided in the CDD/CPD/ORD.

Slide 11

Systems Allocation (Continued)

Sample View

Operational Activity	System	Operational Activity	System	Operational Activity	System
1.2 Evacuate Safety Check	ABV	1.3 Evacuate Navigation Data	ABV	1.4 Control Branching Subsystems	ABV
1.5 Control Vehicle Drive Unit	ABV	1.6 Control Vehicle Drive Unit	ABV	1.7 Coordinate With Other Units	ABV
1.8 Coordinate With Other Units	ABV	1.9 Coordinate With Other Units	ABV	2.0 Perform Manual Events	ABV
2.1 Coordinate With Other Units	ABV	2.2 Evacuate Navigation Data	ABV	2.3 Control Branching Subsystems	ABV
2.4 Control Vehicle Drive Unit	ABV	2.5 Control Vehicle Drive Unit	ABV	2.6 Coordinate With Other Units	ABV
2.7 Coordinate With Other Units	ABV	2.8 Coordinate With Other Units	ABV		

ABV SV-5

Operational Activity to Systems Function Traceability Matrix is a specification of the relationships between the set of operational activities applicable to an architecture and the set of system functions applicable to that architecture. SV-5 depicts the mapping of operational activities to system functions and thus identifies the transformation of an operational need into a purposeful action performed by a system.

In the brief:

- Point out any difficult or complex mappings (non-standard activities or functions).

Slide 12

Systems Integration and Interface Analysis

Sample View

System	Interface	Direction	Frequency	Format	Protocol	Medium	Priority	Security	Access	Control	Management	Operational	Performance	Reliability	Availability	Interoperability	Compliance	Other
ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV	ABV

SV-6 Example from TEG Information

The Systems Integration and Interface Analysis begins to look in greater detail at the specific system interfaces to the system being acquired. The System Information Exchange Matrix (SV-6) from the ISP provides the details needed for this portion of the ISP Establishment Review.

The System Information Exchange Matrix describes (in tabular format) information exchanges between systems. The focus is on how the data exchanges are (or will be) implemented, in system-specific details covering such characteristics as specific protocols, and data or media formats. The SV-6 can potentially be multiple pages in length. Do not try to insert the entire SV-6 into the brief. Provide a synopsis of the matrix, and pull some potential problem or issue areas from the matrix and insert them into the brief.

In the brief be prepared to address the following issues:

- Identify the connectivity components based on requirements in the CDD/CPD/ORD, or non-CDD/CPD/ORD sources.
- Are the project officers for the communication systems noted in the matrix aware of any new interfaces, and message exchanges that will be passed through/to their systems?

<p>Slide 13</p>	<h3 style="text-align: center;">Systems Evolution Description</h3> <p style="text-align: center;">SV-8 Example from JWARN Information</p>	<p>The Systems Evolution Description captures evolution plans that describe how the system, or the architecture in which the system is embedded, will evolve over a lengthy period of time.</p> <p>This information is not specifically addressed in the ISP, but this slide offers the PM an opportunity to explain how the new system fits into the architecture amongst existing systems. The information is obtained from the functional area SV-8 provided by the Product Group SV-8.</p> <p>In the brief, be prepared to address the following issues:</p> <ul style="list-style-type: none"> What system(s) does this system replace, and when? What system(s) will be replacing this system, and when? What significant changes are anticipated?
<p>Slide 14</p>	<h3 style="text-align: center;">Standards</h3> <p style="text-align: center;">Sample TV-1 from the TEG C4ISP</p>	<p>The Specifications addressed in the ISP Establishment Review should be based on the information provided in the Technical Standards Profile (TV-1) from the ISP. IA&JR, in consultation with the program office, normally creates the TV-1 for insertion into the ISP. The TV-1 lists the DISRonline Standards (or other source of standards) needed for interoperability with the systems shown in the SV-2 diagram. As is the case of the SV-6, the TV-1 can potentially be multiple pages in length. Do not try to insert the entire TV-1 into the brief. Provide a synopsis of the matrix, and pull some potential problem or issue areas from the matrix and insert them into the brief. DC C4/I will be particularly interested in references to the mandated common systems, message standards, and data structure shown in the TV-1.</p> <p>In the brief be prepared to address the following issues:</p> <ul style="list-style-type: none"> How/Where are common systems used in the architecture as noted in the TV-1? How is compliance with DISRonline standards going to be (or was) validated? Where were non-DISRonline standards used, and why? How were the DISRonline standards selected? Plans for migrating to future standards, e.g., IPv6? Was a waiver obtained for use of retired or emerging standards, and why?
<p>Slide 15</p>	<h3 style="text-align: center;">Net Centric Analysis</h3> <p>The EFSS data exchange environment: EFSS FDC and the EFSS Section primarily by single channel radio or voice over cable for Increment 1. Since the EFSS contract will not be awarded until after the MS B decision, fourth quarter FY 2004, it is not currently known how the EFSS IT solution will exchange data.</p> <p>For Increment 2 it is anticipated that the AFATDS will employ legacy message and communications protocols of the GDU to affect this interface. However, AFATDS software does not currently support the employment of the EFSS, but AFATDS software currently supports the GDU protocols for existing C4ISR systems, and will continue to do so for the near future.</p> <p>It is expected that it will take approximately two years to modify AFATDS/GDU software for EFSS. Consequently, fielding the EFSS in FY 2006 will have no impact on the GIG. Full compliance with JTA message and communications standards will occur when EFSS Increment 2 is developed.</p> <p style="text-align: center;">Sample Table from the EFSS ISP</p>	<p>Analysis of the sufficiency of IT and NSS information support needs shall be accomplished in terms of the operational and functional capabilities that are being supported. This analysis requires an understanding of the operational and functional capabilities, and associated metrics to assess and evaluate: organizations; organizational relationships; operational activities; node connectivity and required system data exchanges required to achieve a given capability. Table I-A-1 lists the steps in the ISP information needs discovery and analysis process.</p> <p>In the brief:</p> <ul style="list-style-type: none"> Be prepared to address the GIG connections (KIPs) and net-centric capabilities.
<p>Slide 16</p>	<h3 style="text-align: center;">Testing</h3> <ul style="list-style-type: none"> •SoST •FY04 •FedOS •FY05 •JITC •June 2005 	<p>The Testing slide addresses how the system plays in the annual System of System Test (SoST), Federation of Systems (FedOS) Test, JITC certification, and the other interoperability testing for the system. This information is not specifically addressed in the ISP, but this slide offers the PM an opportunity to explain how the interfaces identified in the ISP were tested. There is no specific format offered for this slide.</p> <p>In the brief:</p> <ul style="list-style-type: none"> Be prepared to address if any connections shown in the ISP views were NOT tested, or are not scheduled to be tested. Consider addressing how the SIE (at MCTSSA) was (or will be) used for testing the connectivity to the system being acquired, and is (or will be) resourced with a system for future FedOS testing.

Slide 17

Issues

Operational Issues				
Mission				
Functional Capabilities Impacted				
Issue Number	Supporting System	Issue Description	Issue Impact	Mitigation Strategy/Resolution Path (and Time Frame)
U-1				
S-1				
Development Issues				
Testing Issues				
Training Issues				

Sample View

Example ISP Issues

The Issues addressed in the ISP Establishment Review should be based on the information provided in the table of the last chapter of the ISP. Titled “Issue Summary” the table succinctly lists specific Operational, Developmental, Testing, and Training issues that might affect the development, operation, testing, or training of the system being acquired.

The listed systems or items addressed during this portion of the brief should correspond to the systems identified in the SV-2 graphic. The specifics of the issue should be briefly explained, as well as the method for addressing the risk. The Issue number indicates if the issue is (C)ritical or (S)ubstantive.

In the brief be prepared to address the following:
 A complete explanation of each of the issues
 The anticipated plan of action to address the issues
 Actions taken to date for resolving the issues.

Slide 18

Interoperability Risk Reduction

	R	Y	G
1. System-to-System Interfaces			
a. System 1 Interface Assessment			
b. System 2 Interface Assessment			
c. Etc.			
2. Concurrence by other PM Offices			
a. System 1 Concur/Non-Concur			
b. System 2 Concur/Non-Concur			
c. Etc.			

System Engineer Effort

- Use of SIE
- Training Systems

The Interoperability Risk Reduction slide indicates an assessment of the ongoing effort to ensure interoperability with the systems in the architecture. Three aspects are addressed: An assessment on achieving interoperability, a concurrence on the interface (with the PM of the system), and the system engineering effort being taken to prove the interoperability.

The system-to-system interface assessment, and the concurrence by other PM offices should be indicated by a Red, Yellow, or Green highlighted stoplight.

In the brief:
 Be prepared to address how future (or completed) testing supports the information presented on this slide.

Slide 19

Summary

-
-
-
-

The Summary page of the brief offers an opportunity to the PM to address other issues that don't fit into the format of the ISP Establishment Review. Re-emphasis of issues addressed earlier in the brief would be acceptable for this slide as well. The format for this slide is free text, with bullet leaders.

ATTACHMENT G-2: PROCEDURES FOR THE USE OF NON-MARINE CORPS ISPs

G-2.1 Purpose

This attachment provides the procedures to follow for ISPs developed for systems outside of the Marine Corps, i.e. use of Joint/Other Service programs' ISPs, including procedures to follow when no or inadequate ISPs exist. This includes programs owned by other Services that are used by the Marine Corps.

G-2.2 Background

Procedures for reviewing or validating non-ACAT I-program ISPs, developed by Joint or other Services, are unclear. For ACAT I or IA programs, reference (i) provides review procedures for ISPs submitted to the JCPAT-E and includes the release of those documents to the Services for staffing. Current practices for lower ACAT programs appear to lean towards developing Joint ISPs through an IPT-like process, with the lead DoD Component having the final say on the appearance and specificity of the architecture depictions in the ISP. This process tends to broad-brush the interconnectivity and interoperability of the systems being acquired, and leaves Marine Corps systems poorly represented in the architecture depictions and subsequent program planning.

G-2.3 Procedures

In order to mitigate the potential shortcomings of Joint/Other Services' ISPs, the following procedures will be followed whenever possible:

- a. When a Joint/Other Service ISP is sent to MARCORSYSCOM for review, cognizant PMs receiving the ISP will forward a copy of it to the IA&JR Division for concurrent review.
 - 1) If adequate architectural views are provided, these will be used by IA&JR to meet the ISP requirements, and also forwarded to C4I SE&I for incorporation into the MCIAP.
 - 2) If during the IA&JR or PM support team review, shortcomings are identified in the Marine Corps depictions in the ISP, the PM will consolidate and forward appropriate comments to the Joint/Other Service Program Office. The ISP or 2681 templates available on MCASE offer PMs an ideal tool to communicate correct Marine Corps architecture depictions.
- b. Where there is no attempt by the Joint/Other Service Program Office to provide the needed Marine Corps architecture depictions in the Joint/Other Service ISP, or where no ISP or C4ISP exists, PMs are expected to independently develop the DoD Architecture Framework System Views (SV) SV-2, SV-6 and SV-8 depictions and obtain a Technical View (TV) TV-1 depiction from IA&JR commensurate with their program, and provide them to IA&JR Division. The SV and TV depictions will be used by C4I SE&I Division to maintain correct architectural views of the systems fielded by MARCORSYSCOM as part of the Marine Corps Enterprise Architecture. At System Security Authorization Agreement (SSAA), or Authority to Operate (ATO) decision reviews, PMs will be expected to provide the SV-2, SV-6, SV-8 and TV-1 (2681) architectural depictions that are specific to Marine Corps requirements. An SSAA or ATO will not normally be approved without the required architectural documentation. The process for handling 2681s are described in Section G.5 of the I&IMP Annex G.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H: NR-KPP DEVELOPMENT PROCESS

H.1 PURPOSE

The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of the exchange. The NR-KPP is a required component of CDDs and CPDs, and is to be included in ISPs for systems without a CDD or CPD. This appendix describes the NR-KPP development and approval process for MARCORSYSCOM programs.

H.2 BACKGROUND

The CJCSI 6212.01 (reference (i)) and the CJCSM 3170.01 (reference (r)) requires the development of NR-KPPs for all IT and NSS that are used to enter, process, store, display, or transmit/receive DoD information. The NR-KPP is a required part of CDDs and CPDs (also known as JCIDS documents), and is an enclosure to ISPs for systems without a CDD or CPD. The NR-KPP is comprised of four components: compliance with the NCOW-RM, information assurance, GIG KIP declaration, and integrated architecture products.

H.3 NR-KPP POLICY

The following subsections describe the policy on creation and maintenance of MARCORSYSCOM-generated NR-KPPs.

H.3.3.1 When Required

NR-KPPs are required for all ACAT, non-ACAT systems, including AAPs, and fielded systems that connect in any way to the communications and information infrastructure. NR-KPPs will be used to facilitate interoperability and integration among all C4ISR systems. NR-KPPs are not standalone documents, but are required for inclusion in CDDs and CPDs, or in ISPs if an NR-KPP is not contained in a CDD or CPD, e.g. an ORD-based requirement. Joint Staff approved NR-KPPs are required when a system is submitted for JITC certification since they provide the certified requirements against which JITC tests. Note, if a CDD or CPD already exists, then the ISP will refer to the NR-KPP contained in the CDD or CPD, and a separate NR-KPP is neither required nor desired.

H.3.3.2 NR-KPP Timeframe

When a program meets the criteria specified in CJCSM 3170.01 (reference (r)) requiring a CDD, CPD, or ISP, PGDs and PMs will ensure an NR-KPP is completed/updated prior to major program reviews or milestone decisions.

H.3.3.3 NR-KPP Maintenance

Once completed, an NR-KPP shall be kept current through the final production milestone decision, and updated if undergoing a major upgrade or product improvement, 3-year JITC recertification, or ATO renewal.

H.4 PROCEDURES

The NR-KPP is not a stand-alone document. The NR-KPP is contained in CDDs and CPDs, and in ISPs for systems without a CDD or CPD. MCCDC is responsible for the generation of the CDDs and CPDs, and will lead the development of NR-KPPs for these JCIDS documents. MARCORSYSCOM is responsible for the generation of the ISPs, and will lead the development of NR-KPPs in ISPs for systems without a CDD or CPD.

H.4.1 NR-KPP (JCIDS)

When the NR-KPP generation request originates from MCCDC (i.e., for inclusion in a CDD or CPD), the AVs and OVs are provided by MCCDC, and MCCDC requests MARCORSYSCOM to provide the SVs (generated by the PM) and the TVs (generated by IA&JR). The SVs and TVs are sent back to MCCDC, and the NR-KPP is included in the JCIDS document. Figure H-4-1 provides a diagram of the process used to create NR-KPPs for JCIDS documents (CDDs and CPDs), with MARCORSYSCOM tasks numbered, referring to the procedures described below.

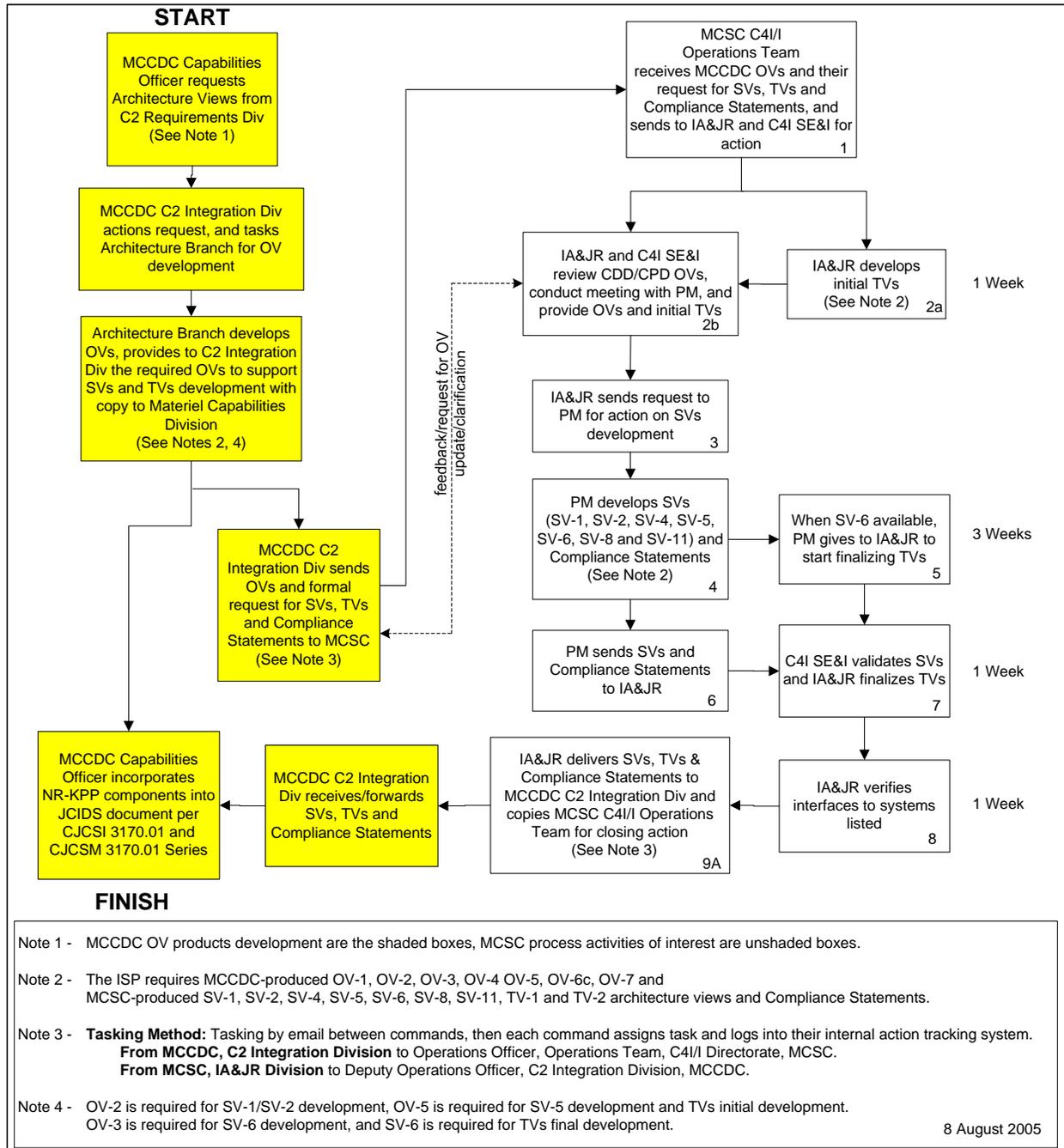


Figure H-4-1: NR-KPP Development Process (JCIDS)

H.4.2 NR-KPP (ISP)

When the NR-KPP generation request originates from MARCORSYSCOM (i.e., for inclusion in an ISP), the AVs, OVs, and capstone requirements documents (CRD) crosswalk are generated by MCCDC and provided to the PM; the SVs are generated by the PM, and the TVs are generated by IA&JR. Figure H-4-2 provides a diagram of the process used to create NR-KPPs for ISPs (when required), with MARCORSYSCOM tasks numbered, referring to the procedures described below.

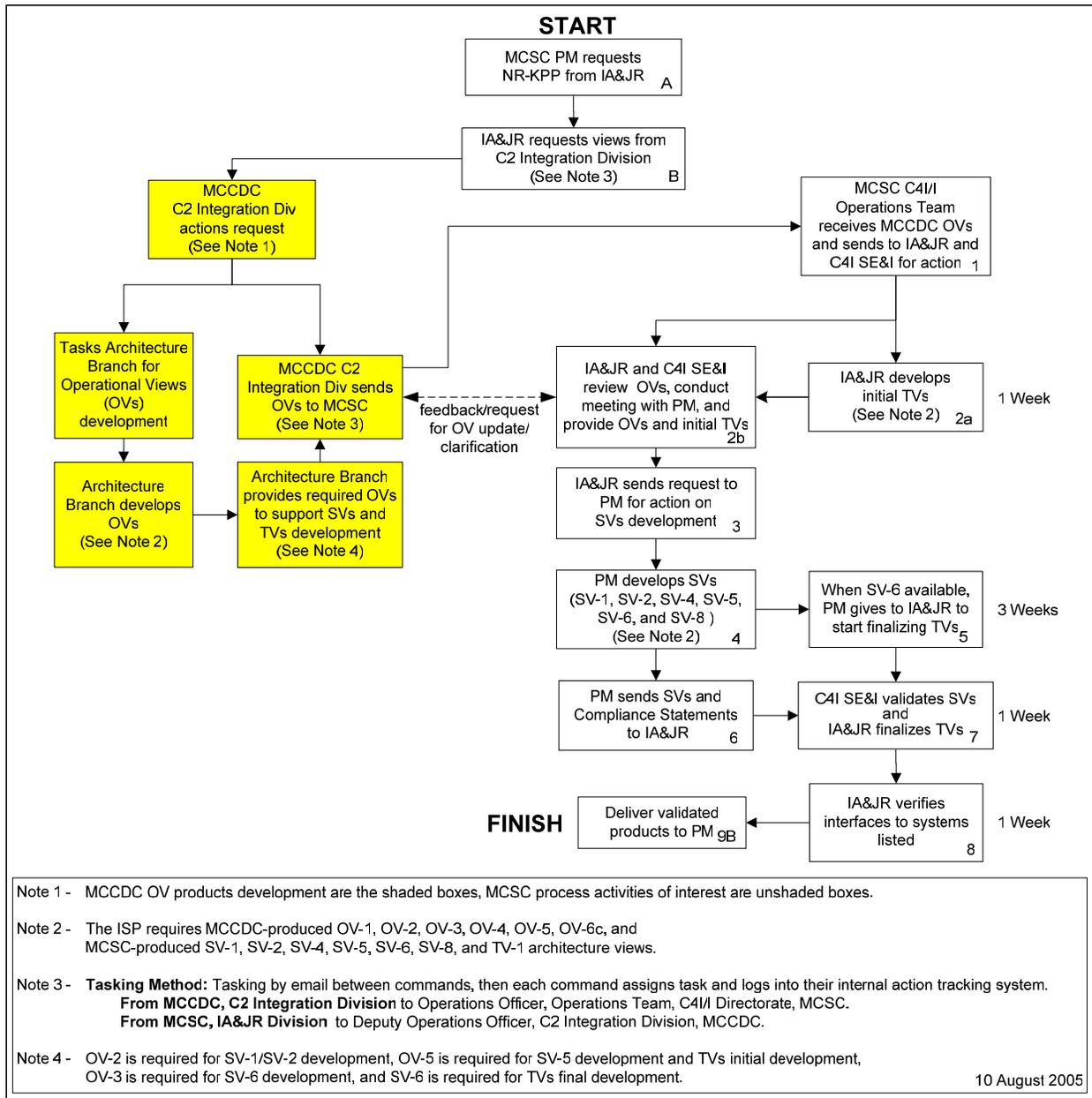


Figure H-4-2: NR-KPP Development Process (ISP)

Note: Both processes are similar, replicating many of the same procedures in both processes. The differences between the two include who is responsible to start the process, and how the

process ends. Unique, differing steps are identified by capital letters in the two figures, e.g., A, B, 9A and 9B. NR-KPPs for inclusion in a JCIDS document, Figure H-4-1, starts with MCCDC, staffs only architecture views to interfacing PMs in Step 8, and completes for MARCORSSYSCOM in Step 9A with the products being delivered to MCCDC. NR-KPPs for inclusion in an ISP, Figure H-4-2, starts with MARCORSSYSCOM in unique Steps A and B, staffs the entire ISP to interfacing PMs in unique Step 8, and completes with delivery of validated products to the PM in unique Step 9B. A detailed description of each step is given below.

H.4.3 NR-KPP JCIDS/ISP Process Description

H.4.3.1 Step A. PM requests NR-KPP from IA&JR (unique to NR-KPP (ISP))

MARCORSYSCOM PM sends a request for MCCDC components of the NR-KPP to DIR IA&JR via email.

H.4.3.2 Step B. IA&JR requests views from C2 Integration Div (unique to NR-KPP (ISP))

DIR IA&JR sends an email to Deputy Operations Officer, C2 Integration Division, MCCDC requesting task to obtain products be appropriately distributed.

H.4.3.3 Step 1. C4I/I Operations Team receives MCCDC OVs and CRD Crosswalk and sends to IA&JR & C4I SE&I for Action.

MCCDC sends the OVs and the CRD crosswalk to MARCORSSYSCOM C4I/I Operations Team, who passes them to IA&JR & C4I SE&I for action. If the NR-KPP is for a JCIDS document, MCCDC will additionally send a request for the SVs, TVs, and compliance statements.

H.4.3.4 Step 2a. IA&JR Develops Initial TVs.

DIR IA&JR uses the OVs provided by MCCDC, as well as the current system architecture, to develop initial TVs for use by the PM.

H.4.3.5 Step 2b. IA&JR and C4I SE&I review OVs and CRD Crosswalk, conduct meeting with PM, and provide OVs and initial TVs.

DIR IA&JR conducts a meeting with the PM, MCCDC, and C4I SE&I once the OVs are received from MCCDC. The purpose of the meeting will be to review the OVs, and CRD Crosswalk if NR-KPP is for an ISP, and establish a timeline for development of SVs and compliance statements. The PM will also receive the initial TVs from DIR IA&JR.

H.4.3.6 Step 3. IA&JR sends request to PM for action on SV development.

DIR IA&JR formally tasks the PM (via the PGD) after the meeting, using the MARCORSSYSCOM tasker system, to develop the SVs and compliance statements.

H.4.3.7 Step 4. PM Develops SVs and Compliance Statements.

PM produces the SVs and the compliance statements in this step of the NR-KPP process. The PM should obtain the current ISP template from MCASE for help in developing DOD Architecture Framework-compliant views. See Attachment H-1, and also the ISP template, for help in compliance statements and their associated efforts.

H.4.3.8 Step 5. When SV-6 available, PM gives to IA&JR to start finalizing TVs.

PM provides the SV-6 to DIR IA&JR once developed, in order to finalize the TVs. DIR IA&JR will work with the PM to develop agreed-upon standards for the system.

H.4.3.9 Step 6. PM sends SVs and Compliance Statements to IA&JR

The PM provides the remaining SVs and compliance statements to DIR IA&JR.

H.4.3.10 Step 7. C4I SE&I validates SVs and IA&JR finalizes TVs. DIR IA&JR finalizes the TVs and send the SVs to C4I SE&I for validation. Comments and change recommendations will be provided back to the PM. The use of DISR standards designated as "Retired" on a TV-1 will require a waiver from DC C4I/I. The waiver request shall be submitted with the NR-KPP. The format for the waiver is available on MCASE. The use of DISR standards designated as "Emerging" will be contained in the TV-2.

H.4.3.11 Step 8. IA&JR verifies interfaces to systems listed
DIR IA&JR staffs the architecture views to the remainder of IA&JR and C4I SE&I once the SVs and TVs are validated. IA&JR will verify the system interfaces by any combination of the following methods:

- a. Verification through analysis of existing approved MOAs, Interface Requirements Specification (IRS), or Interface Design Description (IDD) provided by the PM specific to any of the interfaces identified.
- b. Verification through analysis of existing approved architectural products for interfacing systems available in MCASE, DARS, and/or JCPAT-E.
- c. Routing of architectural views to PMs of interfacing systems for comments/concurrence.

Comments and change recommendations will be provided back to the PM for resolution.

H.4.3.12 Step 9A. IA&JR delivers SVs, TVs, and Compliance Statements to MCCDC and copies C4I/I Operations Team for closing action (unique to NR-KPP (JCIDS))

DIR IA&JR emails the validated SVs, TVs and compliance statements to MCCDC C2 Integration Division, and copies MARCORSSYSCOM C4I/I Operations Team to close the action.

H.4.3.13 Step 9B. IA&JR delivers validated Architecture Views to PM (unique to NR-KPP (ISP))

DIR IA&JR deliver validated SVs and TVs to the PM for inclusion in the NR-KPP, and subsequent addition to the ISP.

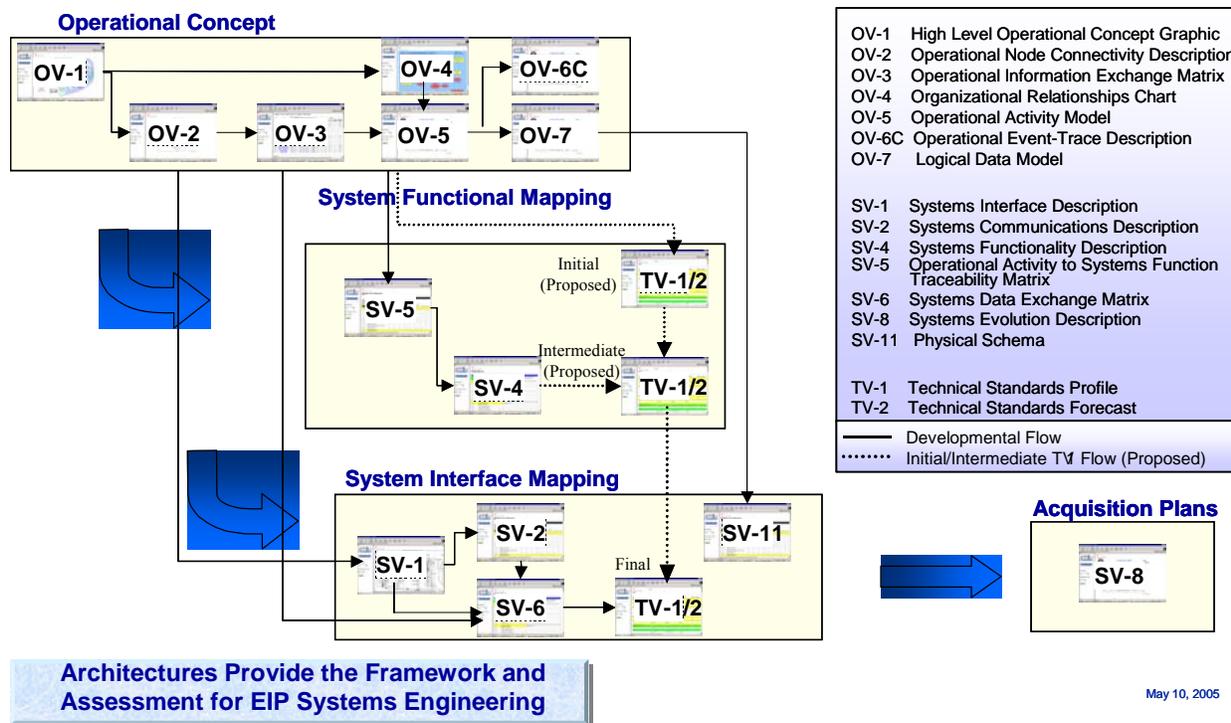
H.5 DEVELOPING COMPONENTS

OV components are developed by MCCDC and provided to the PM. The PM develops SV components using the ISP template provided by IA&JR. IA&JR develops the TVs in coordination with the PM. Figure H-4-3 shows the relationships between the architecture products.

- a. The OV-2 is required for SV-1 development, OV-3 is required for SV-6 development, OV-5 is required for SV-5 development, and OV-7 is required for SV-11 development.
- b. The DoN/USMC Common System Function List (CSFL) shall be used as the basis for the SV-4 and SV-5, which can be found in the Marine Corps Transformational Communications Architecture (MCTCA) Handbook located on MCASE.
- c. In addition to the views required by Joint directives, the OV-3 and SV-8 are required for Marine Corps systems.
- d. The compliance statements can be found in the ISP template.



Using Architecture Products in Systems Engineering & Acquisition



Architectures Provide the Framework and Assessment for EIP Systems Engineering

May 10, 2005

Figure H-4-3: DoDAF Architecture Product Flow

H.6 RESPONSIBILITIES

- a. MCCDC responsible for:
 - Development of AV-1, OV-1, OV-2, OV-3⁺, OV-4, OV-5, OV-6C and OV-7[#];
 - Providing a CRD Crosswalk^{*}.
- b. PM responsible for:
 - Development of SVs from approved OVs, to include SV-1, SV-2, SV-4, SV-5, SV-6, SV-8⁺ and SV-11[#];
 - Development of Compliance Statements^{*} (See Attachment H-1);
 - Ensuring that the system complies with the approved Key Interface Profiles (KIPs) that are declared in the NR-KPP;
 - Provide POC information, MOA and/or IRS/IDD for interfacing systems.
- c. IA&JR responsible for:
 - Providing guidance in the development of architecture views;
 - Verifying SVs;
 - Development of TV-1 and TV-2[#], and associated IT Standards Profile entry into DISRonline^{*};

⁺ Marine Corps-required architectural products, to be submitted with NR-KPP, but not included with the NR-KPP.

[#] Required in CDDs (Milestone B) and in CPDs (Milestone C)

^{*} While not a component of the NR-KPP, they are required.

- System registration in JCPAT-E* ;
- General support to the PM for developing products;
- Obtaining concurrence from PMs of connected systems.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT H-1: COMPLIANCE STATEMENTS AND ASSOCIATED EFFORTS

Compliance statements, though not a part of the NR-KPP, are required for submission with the NR-KPP for JCIDS documents. These compliance statements are for the following:

- E3 and Spectrum Supportability
- Host Nation Approval
- JTRS ORD
- GPS PPS and SAASM

Note: The draft CJCSI 6212.01D eliminates the compliance statements from the ISP, but the following information is valuable as the CJCSM 3170.01B directs the Services to address these in the CDD and CPD.

Electromagnetic Environmental Effects (E3) and Spectrum Supportability

Electromagnetic Environmental Effects (E3) is the discipline of analyzing and managing friendly, unintended adverse electromagnetic interactions and susceptibilities. E3 can impact information availability and integrity and must be appropriately managed.

Spectrum Management (SM) is the discipline of managing the use of the electromagnetic spectrum to prevent mutual interference among the users. SM ensures bandwidth integrity and availability for information exchange. The major components of SM are spectrum certification (SC) and frequency assignment. SC is the process (called the JF-12 Process) by which spectrum-dependent systems/equipment are certified to operate in a portion of the electromagnetic spectrum. Frequency assignment is the operational process that gives the users the authority to operate a fielded, spectrum-dependent system at specific locations on assigned frequencies within the allocated frequency band. E3 and SM are parallel disciplines.

To determine if your system will be affected by E3 requiring an E3 and Spectrum Supportability Statement, the following guidance is provided. If the system will be adversely affected by hostile actions such as electronic surveillance, electronic countermeasures, electromagnetic pulse from nuclear or directed energy weapons, electro-optic countermeasures, or you are unsure, include an E3 and Spectrum Supportability statement. If not, then if the system must demonstrate electromagnetic compatibility with itself and other systems in the operating environment to include such items as the hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning, electrostatic discharge and precipitation static, or you are unsure, include an E3 and Spectrum Supportability statement. Refer to MIL-STD-461, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, and MIL-STD-464, Electromagnetic Environmental Effects Requirements for Systems, for complete definitions, or check with AC PROG for more information.

To determine if your system will be affected by SM requiring an E3 and Spectrum Supportability statement, the following guidance is provided. If the system will transmit or receive in any portion of the electromagnetic spectrum, or you are unsure, include an E3 and Spectrum Supportability statement. The Marine Corps requires all systems that use any portion of the electromagnetic spectrum to submit a DD-1494, Application for Equipment Frequency Allocation, to document its use. Refer to MIL-STD 461 and 464 for complete definitions, or check with AC PROG for more information.

The following is a potential statement for E3 and Spectrum Supportability. All {Program Name} electronic components and subsystems shall be self-compatible and mutually compatible within

themselves and with the operational electromagnetic environment (EME). All {Program Name} spectrum-dependent equipment shall comply with applicable DoD, National and International spectrum management policies and regulations and obtain spectrum certification.

Host Nation Approval

Host Nation Coordination (HNC) is required for spectrum-dependent equipment (specifically, transmitters) prior to the introduction into the host nation. HNC is the process by which spectrum-dependent equipment is approved for use in foreign countries. This coordination is normally part of the national frequency certification process. Upon submittal to the Spectrum Planning Subcommittee, a releasable copy of the DD Form 1494 is provided to the COCOMs and Department of State for submittal to the nations designated in the application. In countries under the purview of a COCOM, the COCOM J6 is responsible for the required coordination. In other countries, the Department of State is responsible for the required coordination activities. Action by the host nation is reported through frequency management channels to the system program office. Strict compliance with all host nation restrictions is mandatory. Deployments of United States military C4I assets to foreign nations have resulted in the denial to operate these assets and even confiscation due to lack of SC, that is, Host Nation Approval (HNA). Host nations have denied frequency assignments to DoD systems because of the electromagnetic interference (EMI) caused to the in-country telecommunication systems. These may be, for example, cellular and other mobile phones, civil aviation, civil defense, other civil and Government systems, meteorological sensors, radar, military systems, and satellite communications.

The DD Form 1494 is used to facilitate the SC review process and begin the coordination with Host Nations. Requests for spectrum supportability assessments shall include identification of those Host Nations into which deployment is likely or planned. Host Nations are those sovereign nations, including the United States, in which the Department of Defense plans or is likely to conduct military operations with the permission of that nation. While an actual determination of spectrum supportability for a spectrum-dependent system within a particular country (i.e., Host Nation) may be possible based upon "spectrum supportability" (e.g., equipment spectrum certification) comments provided by that Host Nation, the overall determination of whether a spectrum-dependent system has spectrum supportability is the responsibility of the MDA based upon the totality of spectrum supportability comments returned from those Host Nations whose comments were solicited.

The following is a potential statement for Host Nation Approval. The DD Form 1494, Application for Equipment Frequency Allocation, documents the operational frequency band(s), planned deployment information, technical characteristics, and performance data of radio frequency (RF) equipment. The data are used by national and international frequency allocation authorities to determine whether or not to permit intentional emissions from the RF equipment, by the Military Communications-Electronics Board for coordination with host (foreign) nations where {Program Name} equipment may be deployed and by military commanders to ensure RF-compatible operation of RF emitter/receivers during military operations

JTRS ORD

Considered a pivotal Department of Defense (DoD) transformational program, the Joint Tactical Radio System (JTRS) is a Defense Department-wide initiative to develop a family of revolutionary software-programmable tactical radios that will provide the warfighter with voice,

data and video communications, as well as interoperability across the joint battlespace. Current radio systems lack interoperability across the spectrum and have insufficient bandwidth to meet present and future communications challenges. The solution for interoperability is an all-service radio and a new wideband networked waveform with the ability to provide mobile networked-connectivity across the battlespace while providing compatibility with the current waveforms in use by the DoD today.

Being the all-service interoperability solution for radios, the Joint Staff wants to ensure that all systems comply with this unifying effort. As such, a JTRS waiver is required if your program desires to purchase a radio that is not software compliant with JTRS.

The following is a potential statement for JTRS ORD. The {Program Name} does/does not include a requirement for radio-based communications. {If yes,} The ISP clearly states that the system will be satisfied by use of software compliant radios in accordance with the Joint Tactical Radio System (JTRS) ORD.

GPS PPS and SAASM

The Global Positioning System (GPS) Precise Positioning Service (PPS) incorporates classified system security functions that consist of Selective Availability (SA), Anti-Spoofing (A-S), and associated cryptography. The GPS PPS security functions are implemented in both hardware and software. Hardware implementations of the GPS PPS security functions are embodied in a family of integrated circuits known generically as GPS security devices. GPS security devices include the PPS Security Module (PPS-SM), Auxiliary Output Chip (AOC), combined PPS-SM/AOC device, Selective Availability Anti-Spoofing Module (SAASM), and SAASM Code Block (SCB). As the next generation security device, SAASM enhances the system security of GPS PPS. SAASM's are being developed by US industry under the cognizance of the GPS Joint Program Office (JPO). GPS PPS Host Application Equipment (HAE) are applications of electronic products that contain any of the GPS PPS security functions. To protect the GPS PPS security functions, GPS security devices and PPS HAE must be controlled to preclude unauthorized access, tampering, theft, or loss.

Accordingly, the Department of Defense (DoD) has assigned to the GPS JPO the overall responsibility for controlling the development, production, sale, and distribution of GPS security devices and PPS HAE. To ensure GPS security requirements are satisfied, DoD policy requires all US Government organizations and US companies to coordinate with the GPS JPO prior to undertaking any development, production, sale, and/or procurement of GPS security devices or PPS HAE. Additionally, the GPS JPO is responsible for reviewing and approving the designs of U.S.-developed GPS PPS HAE to ensure compliance with GPS security requirements.

The following is a potential statement for GPS PPS and SAASM. The {Program Name} does/does not include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS). {If yes,} The ISP clearly states that the system will develop and procure only selective availability anti-spoofing module (SAASM)-based equipment after 1 October 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I: CERTIFICATION AND ACCREDITATION PROCESS

I.1 Purpose

This document summarizes the basic steps to complete the C&A process on any DoD AIS through the Information Assurance (IA) Division of the Marine Corps Systems Command. This process applies to all Top Secret General Service (GENSER) and below information systems.

I.2 Background

The Department of Defense (DoD) Directive 8500.1 mandates the accreditation of DoD Automated Information Systems (AIS) in accordance with DoD Instruction 5200.40, which establishes the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) as the standard Certification and Accreditation (C&A) process for the DoD.

The C&A process should begin pre-Milestone A, in parallel with the system acquisition strategy. A legacy system will enter the process when it requires re-accreditation, validation or when it changes in such a manner that its security posture is impacted.

The System Security Authorization Agreement (SSAA) or Application Security Plan (ASP) is a living document that formalizes agreements regarding all accreditation requirements and the plan to achieve full system accreditation. It is used from the start of the system's lifecycle to specify requirements, guide security actions, maintain operational system security, document risks, identify certification level of effort, and other C&A activities. If another Service/Agency is leading the accreditation effort, the project officer should leverage from the documents originated by that leading Service/Agency.

I.3 C&A Process

The following steps describe the C&A process to be followed for any Marine Corps Systems Command system. These steps are depicted in figure I-1.

1 Registration

Using the IA Registration link on the website, register your system to initiate the Certification and Accreditation Process. http://www.marcorsyscom.usmc.mil/sites/ia/documents/IA_form.html

Fill out the form and click on submit. An IA representative will contact you to set up a meeting to conduct the Certification Requirements Review.

2 Certification Requirements Review (CRR)

This meeting establishes initial contact between the Certification Authority (CA), the Program Manager (PM)/Project Officer (PO), and the User Representative to address certification requirements. During this meeting, a methodology for meeting all requirements, establishing security solutions, managing the IS security activities, and the required documentation will be determined. Applicability to the Clinger Cohen Act, Information Support Plan (ISP), Marine Corps Network Operations and Security Center (MCNOSC.) Authority to Connect (ATC), Information Technology for the 21st Century (IT-21), Information Assurance Vulnerability Alert (IAVA) Management, Secret Internet Protocol Router Network (SIPRnet), and the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 will also be addressed. Attachment I-1 outlines tasks for this meeting.

3 Access to SSAA and ASP Templates

Visit the IA website to request access to security documentation templates. Non-“dot mil” (.mil) e-mail accounts will require a government POC. <http://www.marcorsyscom.usmc.mil/sites/ia>.

4 SSAA or ASP Development by PM

The PM, working in coordination with their technical experts and developers, will draft security documentation. The PM will provide an accreditation package with all required documentation to the IA representative for review. The IA representative will assist PM with SSAA/ASP development as necessary. This becomes an iterative process between the developer of the documentation and the IA Team.

5 IA Review

The IA Team will conduct a formal technical review and evaluation of the security package to establish compliancy with specified security requirements. The IA Team will identify any deficiencies and provide recommendations and requirements necessary to achieve full accreditation. When it is determined that an Interim Approval to Operate (IATO) is to be issued due to deficiencies, the PM is required to develop a milestone plan with dates to correct the deficiencies noted in the certification report. This must be completed and submitted prior to issuance of an IATO. All required security tests and evaluations must be completed prior to final security package submission for an Authority to Operate (ATO). The final security package must also include the signature of the PM and User Representative prior to submission for CA Approval.

6 CA Approval

After reviewing the package, the CA will make a recommendation to the Designated Approving Authority (DAA) to grant either:

- Full accreditation or Authority to Operate (ATO)
- Interim Approval to Operate (IATO)
- Accreditation disapproval

7 DAA Approval

Upon receipt of the CA's approval recommendation, the DAA will meet with the PM and IA representative to sign the IATO or ATO. An ATO is a full accreditation and is issued for a period not to exceed three years. It is the responsibility of each PM to ensure their assets obtain formal accreditation or cease operation. An IATO is temporary in nature and will be issued for up to 180 days. No more than two IATOs will be issued by the DAA.

I.4 Checklists

Review the Marine Corps Systems Command (MARCORSYSCOM) Information Assurance Certification Requirements Review guide at Attachment I-1, the Certification & Accreditation (C&A) Check-Off Sheet at Attachment I-2, and the SSAA Preparation Checklist at Attachment I-3 to help guide you through the Security Certification & Accreditation Process. You can also obtain additional information and references at the IA website:

<http://www.marcorsyscom.usmc.mil/sites/ia>.

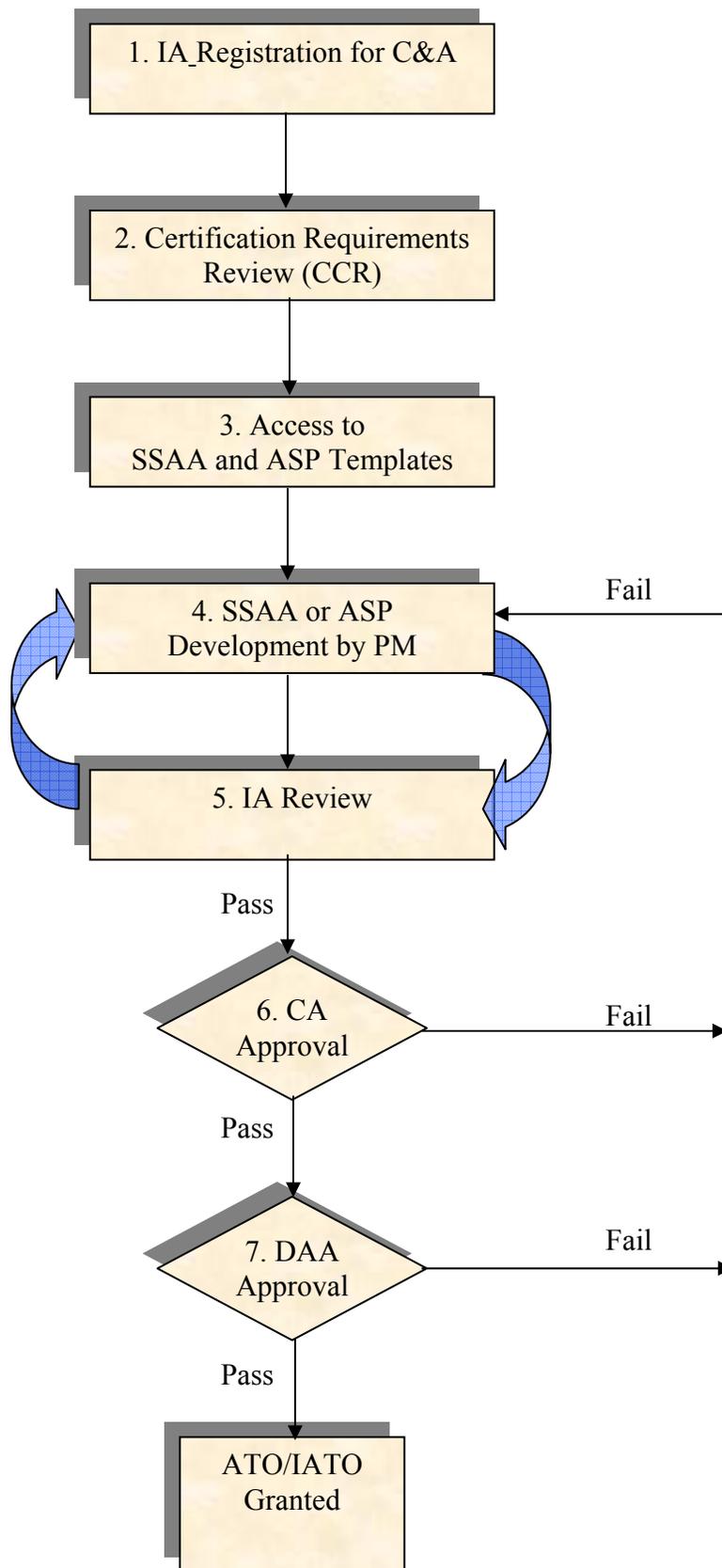


Figure I-1: Certification and Accreditation (C&A) Process

THIS PAGE INTENTIONALLY LEFT BLANK

**MARINE CORPS SYSTEMS COMMAND INFORMATION ASSURANCE
CERTIFICATION REQUIREMENTS REVIEW**

DATE CONDUCTED: _____

IN ATTENDANCE:

PM REP: _____

USER REP: _____

CA REP: _____

TASK 1

System Description (i.e. What does system do?) _____

Connectivity: SIPRnet / NIPRnet (Please circle)

Shipboard (IT-21 or other) Requirement: YES / NO (Please circle)

Have you identified security requirements from an ORD, CDD, CPD, or other related system documentation? If so, identify the document.

Certification Level determination: 1 2 3 4 (Please circle)

Mission Assurance Category (MAC) Level: I II III (Please circle)

Evaluate need for Security Test and Evaluation (ST&E) _____

Required Security Documentation:

- ASP
- SSAA
- Other

TASK 2

Information Assurance Vulnerability Alerts (IAVAs)

Per references (l) and (p), "DoD Component IA programs shall provide the capability to systematically identify and assess vulnerabilities and to direct and track coordinated mitigations. Compliance is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities." Management of this process should include plans to:

- √ Evaluate application/system for IAVA compliance
- √ Ensure existing applications/systems are IAVA compliant
- √ Maintain compliance with IAVA reporting procedures

TASK 3

Understanding of Clinger-Cohen Act (CCA) Requirements

Confirmation of compliance with the CCA has been defined by the DoD as verifying compliance with the following eleven (11) key items. Additional information may be obtained at:

<http://www.marcorsyscom.usmc.mil/ccaweb.nsf/index>.

A determination has been made that:

- ✓ The acquisition supports core, priority functions of the Department
- ✓ Outcome-based performance measures are linked to strategic goals
- ✓ Redesign of the processes that the system supports reduce costs, improve effectiveness and maximize the use of commercial off-the-shelf (COTS) technology
- ✓ No private sector or government source can better support the function
- ✓ An analysis of alternatives has been conducted
- ✓ An economic analysis has been conducted that includes a calculation of the return on investment; or for non-AIS programs, a Life Cycle Cost Estimate (LCCE) has been conducted
- ✓ There are clearly established measures and accountability for program progress
- ✓ The acquisition is consistent with the Global Information Grid (GIG) policies and architecture, to include relevant standards
- ✓ The program has an information assurance strategy that is consistent with relevant DoD policies, standards and architectures. **Note: The IA Strategy should be done in concurrence with the Acquisition Strategy. Recommend submittal six months prior to Milestone Decision.
- ✓ To the extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments
- ✓ The system being acquired has been registered in the DON IT Registry. Do you have a registration number? Yes/No (Please circle)

If yes, what is it? _____

If no, provide required information within thirty-days.

_____ (Initials of PM to show knowledge of deadline.)

TASK 4

Information Support Plan (ISP)

Required for all programs that connect to communications infrastructure in any way. Used to facilitate interoperability and integration among C4I systems.

- Required
- Not Required
- Other (explain): _____

POC Mr. Marty Marbach 540-657-5128 <http://www.marcorsyscom.usmc.mil/sites/sei/>

TASK 5

Authority to Connect to MCEN.

Contact MCNOSC at SPC&A@noc.usmc.mil or visit their website at <https://www.noc.usmc.mil/>

TASK 6

IT-21

To request access to <https://inets.spawar.navy.mil/cmsyshome> IT-21 website or for general questions contact:

CDR Sityar at SityarI@mcsc.usmc.mil / (703) 432-3866 or
Capt Laboy at Laboys@mcsc.usmc.mil / (703) 432-3857.

Posts policy documents, Integrated Shipboard Network System (ISNS) technical documents and briefs from the Network Users Working Group (NUWG) conferences. You can also put in and track your Navy Change Request (NCR) if there is a system that you want IT-21 certified at this site. The SPAWAR Technical Point of Contact for Marine Corps IT-21 NCRs is Alfredo Polanco. Another website of interest for IT-21 is <https://infosec.navy.mil>.

TASK 7

NSTISSP-11

The Committee on National Security Systems (CNSS) policy, National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, governs the acquisition of Information Assurance (IA) and IA-enabled Information Technology (IT) products (reference (q)). To see the policy published in January 2000 and revised in January 2003, go to this site:

http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf

TASK 8

SIPRnet connection

For information and templates on SIPRnet connections, go to this website:

<http://www.disa.mil/ciae/iapage.html>.

Coordinate activities with MCNOSC at DAA@noc.usmc.smil.mil

Project Officer/Program Manager

User Representative

Information Assurance Representative

THIS PAGE INTENTIONALLY LEFT BLANK

**CERTIFICATION & ACCREDITATION CHECK-OFF SHEET
FOR _____**

PHASE I DEFINITION

1. Document Mission Need, when was it drafted/submitted? _____
2. When was Registration started? _____
3. When were Negotiations begun and finished? _____
(Negotiations are completed when all responsible organizations adopt the SSAA)
4. When was an agreement reached? _____
5. Has the initial SSAA been started? _____
6. Who is the supporting Contractor for the SSAA? _____
7. Who is the primary POC at the supporting Contractor for the SSAA? _____

PHASE II VERIFICATION

1. When was the SSAA reviewed and updated? _____
2. Who performed the review of the SSAA? _____
3. When was the System Architecture Analysis performed? _____
4. Who/what Activity performed the System Architecture Analysis? _____
5. When was the Software Design Analysis performed, if required? _____
6. Who/what Activity performed the Software Design Analysis? _____
7. When was Network Connection Rule Compliance Analysis performed? _____
8. Who/what Activity performed the Network Connection Compliance Analysis? _____
9. When was Integrity of Integrated Products Analysis performed? _____
10. When was Life Cycle Management Analysis performed? _____
11. When was Vulnerability Assessment Analysis performed? _____
12. Who/what Activity performed the Vulnerability Assessment Analysis? _____

PHASE III VALIDATION

- 1. Date of System Security Testing and Evaluation completed. _____
 - 1a. Are Test Reports available? _____ (required)
- 2. Was Penetration Testing performed? When? By whom? _____ / _____ / _____
 - 2a. Are Test Reports available? _____ (required)
- 3. Was TEMPEST and Red-Black Verification held, if required? _____ Date _____
 - 3a. Are Test Reports available? _____ (required)
- 4. Was Validation of COMSEC Compliance performed? _____ Date _____
 - 4a. Are Test Reports available? _____ (required)
- 5. Has System Management Analysis been performed? _____ Date _____
(Documentation Required)
- 6. Has a Contingency Plan Evaluation be conducted? _____ Date _____
(Documentation Required)
- 7. Has a Risk Management Review been held? _____ Date _____
(Documentation required)
- 8. Has the CA/DAA's accreditation decision been obtained? _____

PHASE IV POST ACCREDITATION

- 1. Review the SSAA, Obtain approval of changes, if any. _____
- 2. Document any changes to the SSAA, if any. _____
- 3. Perform System Maintenance. _____
- 4. Execute System Security Management. _____
- 5. Conduct Contingency Planning. _____
- 6. Support System Configuration Management. _____
- 7. Conduct Risk-based Management Review. _____
- 8. Perform another SSAA Review. _____
- 9. Perform Physical Security Analysis. _____
- 10. Perform procedural Analysis. _____
- 11. Conduct Another Risk-based Management Review. _____

SSAA PREPARATION CHECKLIST

TASK	ACTIVITY and STEP		
1	Activity: Describe System and Mission	DITSCAP Para #	Date Completed
	Step 1: Write System Description <ul style="list-style-type: none"> • System Name/Mission • Responsible Organization • System Capabilities • System Criticality • Classification Levels and Sensitivity of Data 	DOD: 5200.40 (E3.3) 5200.40-M (1.0-1.3.3)	
	Step 2: Determine User Description <ul style="list-style-type: none"> • Users and Their Roles • Users' Classification Level • Users' Formal Access Approval for Categories 	DOD: 5200.40 (E3.3) 5200.40-M (1.3.4)	
	Step 3: Determine Life Cycle of the System <ul style="list-style-type: none"> • Life Cycle Stage 	DOD: 5200.40 (E3.3) 5200.40-M (1.3.5)	
	Step 4: Determine System CONOPS <ul style="list-style-type: none"> • System Concept of Operation • Other Systems • Place in Section 1 of the SSAA 	DOD: 5200.40 (E3.4) 5200.40-M (1.4)	
2	Activity: Develop Environment Description	DITSCAP Para #	Date Completed
	Step 1: Describe Operating Environment <ul style="list-style-type: none"> • Operating Environment Overview 	DOD: 5200.40 (E3.4) 5200.40-M (2.1)	
	Step 2: Determine Security Requirements <ul style="list-style-type: none"> • Facility Description • Physical/Administrative Security • Maintenance Procedures • Training Plans 	DOD: 5200.40 (E3.4) 5200.40-M (2.1.1-2.1.5)	
	Step 3: Describe Software Development/Maintenance <ul style="list-style-type: none"> • System Development Approach • Information Access • Configuration Control 	DOD: 5200.40 (E3.4) 5200.40-M (2.2)	
	Step 4: Describe System Threats <ul style="list-style-type: none"> • Threat Description • Threat Environment • Place in Section 2 of the SSAA 	DOD: 5200.40 (E3.4) 5200.40-M (2.3-2.3.2)	
3	Activity: Describe System Architecture	DITSCAP Para #	Date Completed
	Step 1: Describe System Hardware <ul style="list-style-type: none"> • Target Hardware and Function • Detailed Equipment List • COMSEC/TEMPEST 	DOD: 5200.40 (E3.5) 5200.40-M (3.1)	
	Step 2: Describe System Software <ul style="list-style-type: none"> • Operating System • Database Management System • Applications • GOTS/COTS 	DOD: 5200.40 (E3.5) 5200.40-M (3.2)	
	Step 3: Describe System Firmware <ul style="list-style-type: none"> • Unique Products • Evaluated Product List (EPL) 	DOD: 5200.40 (E3.5) 5200.40-M (3.3)	
	Step 4: Identify Interfaces and External Connections <ul style="list-style-type: none"> • Purpose of External Interfaces • Diagram of Communications Links • Encryption Techniques 	DOD: 5200.40 (E3.3) 5200.40-M (3.4)	
	Step 5: Describe Data Flow <ul style="list-style-type: none"> • Types of Data • Flow of Critical Information 	DOD: 5200.40 (E3.5) 5200.40-M (3.5)	
	Step 6: Describe DOD TAFIM DGSA <ul style="list-style-type: none"> • Comparison of System Features with the DGSA • Diagram of System Architecture to the DGSA 	DOD: 5200.40 (E3.5) 5200.40-M (3.6)	
	Step 7: Describe System Accreditation Boundary <ul style="list-style-type: none"> • Delineation of Components to be Evaluated in C&A • Include in Section 3 of the SSAA 	DOD: 5200.40 (E3.5) 5200.40-M (3.7)	

SSAA PREPARATION CHECKLIST

TASK	ACTIVITY and STEP		
4	Activity: Determine System Security Requirements	DITSCAP Para #	Date Completed
	Step 1: Determine Security Requirements <ul style="list-style-type: none"> • National • DOD • Office of Management & Budget (OMB) Circulars • Service/Command Requirements • Trusted Computer Security Evaluation Criteria 	DOD: 5200.40 (E3.5) 5200.40-M (5.0-5.1)	
	Step 2: Determine Governing Security Requirements <ul style="list-style-type: none"> • Local Agency Requirements • DAA Requirements 	DOD: 5200.40 (E3.5) 5200.40-M (5.2)	
	Step 3: Determine Data Security Requirements <ul style="list-style-type: none"> • Requirements from Data Owner 	DOD: 5200.40 (E3.5) 5200.40-M (5.3)	
	Step 4: Describe Security Concept of Operations (CONOPS) <ul style="list-style-type: none"> • Security CONOPS • Trusted Facility Manual/Security Feature User's Guide TFM/SFUG 	DOD: 5200.40 (E3.5) 5200.40-M (5.4)	
	Step 5: Describe Network Connection Rules <ul style="list-style-type: none"> • To Connect to This System • To Connect to Other Systems 	DOD: 5200.40 (E3.5) 5200.40-M (5.5)	
	Step 6: Describe Configuration and Change Management <ul style="list-style-type: none"> • Configuration Management Plan 	DOD: 5200.40 (E3.5) 5200.40-M (5.6)	
	Step 7: Define Re-Accreditation Requirements <ul style="list-style-type: none"> • Unique Organizational Requirements • Place in Section 5 of the SSAA 	DOD: 5200.40 (E3.5) 5200.40-M (5.7)	
	Step 8: Determine System Security Requirements <ul style="list-style-type: none"> • Requirements Traceability Matrix (RTM) 	DOD: 5200.40 (E3.5) 5200.40-M (5.8)	
5	Activity: Determine Responsibilities and Resources	DITSCAP Para #	Date Completed
	Step 1: Identify Key Authorities <ul style="list-style-type: none"> • DAA/CA • User Representative/Program Manager/Project Officer 	DOD: 5200.40 (E3.5) 5200.40-M (6.0-6.1)	
	Step 2: Identify Resources Required to Conduct C&A <ul style="list-style-type: none"> • C&A Staffing Requirements • C&A Funding Requirements • Contractor Requirements 	DOD: 5200.40 (E3.5) 5200.40-M (6.2)	
	Step 3: Describe the C&A Training Requirements <ul style="list-style-type: none"> • Types of Training • Developed Equipment 	DOD: 5200.40 (E3.5) 5200.40-M (6.3)	
	Step 4: Describe IA Team Roles and Responsibilities <ul style="list-style-type: none"> • Security Personnel C&A Responsibilities • Security Personnel C&A Accomplishments 	DOD: 5200.40 (E3.5) 5200.40-M (6.4)	
Step 5: Identify Other Supporting Organizations <ul style="list-style-type: none"> • Organizations and Working Groups • Place in Section 6 of the SSAA 	DOD: 5200.40 (E3.5) 5200.40-M (6.5)		
6	Activity: Describe the DITSCAP Plan	DITSCAP Para #	Date Completed
	Step 1: Describe the Tailoring Factors <ul style="list-style-type: none"> • Programmatic Considerations • Security Environment • IT System Characteristics • Use of Previously Approved Solutions 	DOD: 5200.40 (E3.5) 5200.40-M (7.0-7.1.4)	
	Step 1a: System Interface Mode <ul style="list-style-type: none"> • Benign • Passive • Active 	DOD: 5200.40 (E3.5) 5200.40-M (4.1)	
Step 1b: System Processing Mode <ul style="list-style-type: none"> • Dedicated • System High • Compartmented • Multi-Level 	DOD: 5200.40 (E3.5) 5200.40-M (4.2)		

SSAA PREPARATION CHECKLIST			
TASK	ACTIVITY and STEP		
	Step 1c: System Attribution Mode <ul style="list-style-type: none"> • None • Rudimentary • Selected • Comprehensive 	DOD: 5200.40 (E3.5) 5200.40-M (4.3)	
	Step 1d: System Mission-Reliance Factor <ul style="list-style-type: none"> • None • Cursory • Partial • Total 	DOD: 5200.40 (E3.5) 5200.40-M (4.4)	
	Step 1e: System Accessibility Factor <ul style="list-style-type: none"> • Reasonable • Soon • ASAP • Immediate 	DOD: 5200.40 (E3.5) 5200.40-M (4.5)	
	Step 1f: System Accuracy Factor <ul style="list-style-type: none"> • Not Applicable • Approximate • Exact 	DOD: 5200.40 (E3.5) 5200.40-M (4.6)	
	Step 1g: Information Categories <ul style="list-style-type: none"> • Unclassified • Sensitive Information • Collateral Classified • Compartmented/Special Access Classified 	DOD: 5200.40 (E3.5) 5200.40-M (4.7)	
	Step 1h: System Class Level <ul style="list-style-type: none"> • Mathematical Figure Representing Sum of All Weights 	DOD: 5200.40 (E3.5) 5200.40-M (4.8)	
	Step 1i: Classification Analysis Level <ul style="list-style-type: none"> • Statement from the Certifier • Place in Section 4 of the SSAA 	DOD: 5200.40 (E3.5) 5200.40-M (4.9)	
	Step 2: Describe the C&A Tasks and Milestones <ul style="list-style-type: none"> • Activity • Schedule • Estimated Duration • Responsibility for the Activity 	DOD: 5200.40 (E3.5) 5200.40-M (7.2)	
	Step 3: Identify the Schedule Summary <ul style="list-style-type: none"> • Gantt Chart • Time-order 	DOD: 5200.40 (E3.5) 5200.40-M (7.3)	
	Step 4: Describe the Level of Effort for Certification <ul style="list-style-type: none"> • As Determined in Section 4 of the SSAA • Place in Section 7 of the SSAA 	DOD: 5200.40 (E3.5) 5200.40-M (7.4)	

THIS PAGE INTENTIONALLY LEFT BLANK

**APPENDIX J: SYSTEMS ENGINEERING AND INTEGRATION ASSESSMENTS
PROCESS**

TBD

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX K: COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, COMBAT AND INTELLIGENCE SYSTEMS MODERNIZATION PROCESS (C5I MP)

K.1 Purpose

The purpose of this Appendix is to formalize and align Marine Corps Systems Command (MARCORSYSCOM) participation in Naval Sea Systems Command (NAVSEA) C5I Modernization Process in support of Commander Fleet Forces Command (CFFC) Fleet Response Plan (FRP). The C5I MP will ensure earlier availability of critical Fleet Commander assets, influence the Program Objective Memorandum (POM) Process, and increase platform commonality. In turn, the CFFC FRP provides a means to ensure Carrier Strike Group (CSG) and Expeditionary Strike Group (ESG) ships are equipped with certified, operational, and interoperable war fighting C4ISR and combat systems capabilities.

K.2 Background

MARCORSYSCOM became a participant in the Chief of Naval Operations (CNO)-directed, NAVSEA managed, Deployment Minus 30 Months (D-30) Process in FY 00. Within the last year the D-30 process has been replaced by C5I MP and under the purview of the Systems Engineering and Integration (SE&I) Division, Naval Integration Team (NIT), significant progress has been achieved in the area of Navy and Marine Corps C4I systems amphibious interoperability and integration. The NAVSEA C5I Modernization Process provides guidelines as to how Deploying Groups prepare for surge and to deploy. C5I MP has a two-fold purpose for the Marine Corps:

1. MARCORSYSCOM, in coordination with the MARFORs, provides a MAGTF Afloat Baseline (MAB), which includes a Marine Expeditionary Brigade (MEB) C4I systems projected baseline for each ESG.
2. MARCORSYSCOM, in coordination with Marine Corps Combat Development Command (MCCDC), Headquarters Marine Corps (HQMC), and the Marine Forces (MARFORs), identifies shortfalls in Navy amphibious C4I architecture and systems used by embarked Marines, based on MCCDC Letter dated 14 February 2003, Expeditionary C4ISR Requirements, and Lessons Learned from previous deployments. Hardware and software for all MAB systems are tracked by C4I SE&I. This effort has resulted in increased amphibious C4I capabilities for deploying Marine Expeditionary Units (MEUs).

Another important area of progress has been the inclusion of Marines in the Navy Deploying Groups Systems Integration Testing (DGSIT), which occurs about five months prior to ESG deployment.

DGSIT is an underway-stressed operational system integration test of Navy and Marine C4I systems. Marine Corps Tactical Systems Support Activity (MCTSSA) has developed an Expeditionary C4I Scenario Checklist (ECSC) for each MAB system to be used during DGSIT. With anticipated inclusion of DGSIT in the HQMC MEU Pre-deployment Training Plan (PTP), Marines are now an active participant in DGSIT and will focus on the testing of MAB systems as part of an integrated, amphibious expeditionary architecture. The MARFORLANT DGSIT Coordinator is providing timely feedback to MCSC Project Officers regarding DGSIT evolutions. This feedback may be in the form of a request for information or assistance in resolving a DGSIT issue relative to a MARCORSYSCOM program.

K.3 Actions Required

The Naval Integration Team of C4I SE&I provides the primary MARCORSSYSCOM C5I MP interface to NAVSEA and other Navy Systems Commands. Specific responsibilities and actions are as follows:

1. The Deputy Commander C4I Integration will ensure inclusion of information requested in the attached C5I Modernization Process questionnaire during the development of the annual Program Management Plan (PMP) brief for each system.
2. The Product Group Directors and Program Managers will ensure completion of the C5I MP questionnaire for all systems under their cognizance to include posting to the MCASE.
3. The Commanding Officer, MCTSSA, Deputy Director, Operational Forces Support Division (OFSD), will maintain the Master Expeditionary C4I Scenario Checklist (ECSC). Updates to the ECSC will occur subsequent to each PDS and FIT evolution.
4. The Director, C4I Systems Engineering and Integration Division will have the Naval Integration Team representatives provide assistance as required to all PMs in the Tier designation of their systems, inclusion in the MAB, baselining of C4I systems for the C5I Modernization Process, and update of the ECSCs maintained by MCTSSA. C4I system issues discerned during DGSIT, which are relative to MCSC program, will be addressed to the Director, SE&I. The Director SE&I will ensure that prompt responses are provided to the DGSIT Process when feedback or request for assistance is received.

K.4 C5I Modernization Process Questionnaire

To fully engage MARCORSSYSCOM managers in this effort, specific programmatic information is required for each system included in the MAB. A Project Officer’s C5I MP checklist has been developed and provided below, which delineates the needed information. Naval Integration Team representatives will assist Program Managers and Project Officers in the completion of this questionnaire.

- a. Using the MAB Tier definitions given below, identify with which tier this system is associated. If a system is Tier 1, project officer must contact Naval Integration Team C5I MP representative for further guidance on Navy Ship Alteration Process. Tier _____
- b. What is the projected Initial Operational Capability (IOC) date and projected MEF fielding schedule by both fiscal year (FY) and quarter (Qtr)?
 I MEF _____ II MEF _____ III MEF _____
- c. What are the current and projected software versions by quarter, for one year?

System	Current Qtr	Subsequent Qtr	Subsequent Qtr	Subsequent Qtr

- d. On which “L” class ships is this system intended to deploy, e.g. LHA, LHD, LPD, LPD Flag, LSD?

- e. On the ship, at which amphibious Operational Facility (OPFAC) is this system intended to located, e.g. SACC, LFOC, JIC, etc.? _____
- f. If required, does the system have an IATO/ATO and ATC?
 IATO? Y/N _____ If yes, what is the expiration date?: _____
 ATO? Y/N _____ If yes, what is the expiration date?: _____
 ATC? Y/N _____ If yes, what is the expiration date?: _____
- g. Has the MCSC PM/PO reviewed the ECSC system functional checklist for correctness and completeness? Y/N _____
 If so, have recommendations for changes been forwarded to MCTSSA, Deputy Director, Operational Forces Support Division? Y/N _____
- h. Has the MCSC PM/PO reviewed and updated the information for each annual PMP brief? Y/N _____

MAGTF Afloat Baseline (MAB) Tier Definitions

TIER-1N: Navy systems and services that the embarking MAGTF requires installed in order to perform expeditionary operations and missions. These systems are permanently installed aboard ship.

TIER 1: Embarking MAGTF carry-on systems requiring additional permanently installed infrastructure (i.e. power, cables, racks, etc.), which is currently not part of existing ship's infrastructure. System could remain on ship when the Landing Force initially transitions ashore. (e.g. AFATDS, EADS). Tier 1 systems identify disconnects between Marine Corps and Navy-identified requirements. These systems should migrate to a Tier 1N or 2 once a Navy Ship Alteration has been generated and implemented.

TIER 2: Systems which are carried on by an embarking MAGTF and temporarily connected to the existing ship's communications infrastructure. These system transition ashore with the Landing Force. (e.g. IOS, TCAC, MAGTF II).

TIER 3: Systems which the embarking MAGTF brings aboard and deploys ashore during amphibious operations. These systems do not connect to the ship's communications infrastructure except to test or update prior to debarkation. These systems reach back to the ARG during movement ashore and/or when established ashore, and require a compatible system aboard ship for interoperability. (e.g. SINCGARS, TDN, MRC-142 (DWTS)).

THIS PAGE INTENTIONALLY LEFT BLANK

**APPENDIX L: PROCESSES FOR SUPPORT TO GROUPS EXTERNAL TO MARINE
CORPS SYSTEMS COMMAND**

TBD

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX M: URGENT UNIVERSAL NEED STATEMENT (UNS) PROCESS FOR INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

M.1 INTRODUCTION:

The Urgent Universal Need Statement (UNS) program is designed to be responsive and flexible in rapidly identifying and fielding the materiel requirements and logistics support structure for warfighters deployed, or preparing for immediate deployment.

There are cases where Urgent UNS are replacing, upgrading, or increasing existing equipment used by the operating forces, or adding new equipment that is used by other Services. This process is applicable only to IT and NSS, i.e., C4ISR systems. Though this process does not include required logistics support, the Project Officer (PO) should determine and plan for providing the appropriate logistics for equipment fielded under an Urgent UNS, including manpower, training, and material requirements. The PO should leverage off any existing documents prior to developing new documentation outlined below. Use of existing documents must be current.

M.2 REQUIREMENT/PROCESS

Urgent UNS may be developed for several types of acquisitions. Fielding equipment purchased under an Urgent UNS minimally requires an Interim Approval to Operate (IATO); Safety Release; and DD-1494 Application for Equipment Frequency Allocation (if applicable). The process for this is depicted in Figure M-1 and described below.

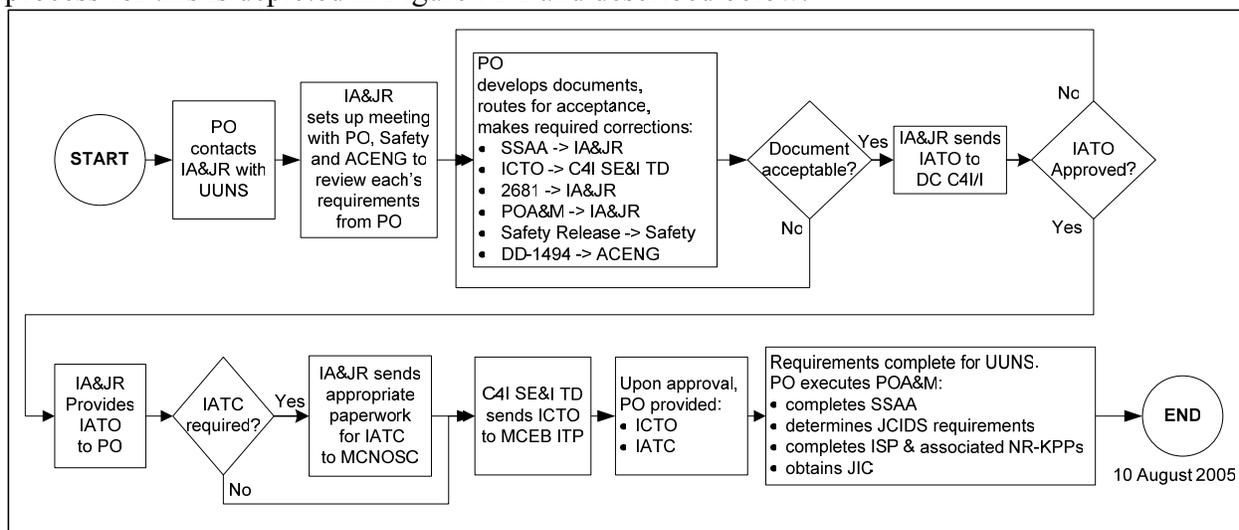


Figure M-1: Urgent UNS Process for C4ISR

M.2.1 Interim Approval to Operate (IATO)

Up to two (2) IATO's can be granted for a maximum of 180 days each. Minimally the following four documents must be completed prior to approving an IATO. If the equipment is going to connect to the MCEN (SIPRnet, NIPRnet), the Information Assurance and Joint Requirements (IA&JR) Division will submit the appropriate paper work to MCNOSC to acquire an Interim Authority to Connect (IATC). The PO requires no action for an IATC.

1) System Security Authorization Agreement (SSAA)

Document template can be found on the C4II Knowledge Center Toolkit/Resources under the "UUNS Universal Needs Statement Toolkit" folder. The PO shall work directly with IA&JR to complete the required sections, as indicated in Table M-1. Submission of the

PO-corrected SSAA, with required sections, fulfills the immediate SSAA requirement for an IATO.

SECTION	TITLE OF SECTION
Chapter 1	Mission Description and System Identification
Chapter 2	Environment Description
Chapter 3	System Architectural Description
Chapter 4	System Security Requirements
Chapter 5	Organizations and Resources
Chapter 6	DITSCAP Plan
Appendix A	Acronyms
Appendix B	Definitions
Appendix C	References
Appendix D	System Concept of Operations/Employment
Appendix F	Security Requirements and/or Requirements Traceability Matrix
Appendix H	Security Test and Evaluation Plan and Procedures
Appendix I – Att 1	Application Interfaces and External Connections
Appendix P	Test and Evaluation Reports
Appendix Q	Residual Risk Assessments Results

Table M-1: Urgent UNS-Required Sections of SSAA

2) Interim Certificate to Operate (ICTO)

The Interim Certificate to Operate (ICTO) Request Form is a document used to obtain an ICTO. An ICTO is an interim, limited time authority to field new systems or capabilities without meeting the Joint Interoperability Certification requirements of DoDD 4630.5/CJCSI 6212.01. ICTOs will not exceed one year.

Document template can be found on the C4II Knowledge Center Toolkit/Resources under the “UUNS Universal Needs Statement Toolkit” folder. The PO will need to fill out the ICTO Request Form and provide it to IA&JR, who will forward it for action to the Test Director (TD) /C4I SE&I. Submission of the ICTO Request Form fulfills the immediate ICTO requirement for an IATO.

The Test Director will present the ICTO to the MCEB Interoperability Test Panel (ITP) and may request support by the PO. The end result will be an approved ICTO with an expiration date. Prior to ICTO expiration, the Program Office will either return for an extension (total time not to exceed 1 year) or be successful in getting JITC Interoperability Certification (JIC), requiring an approved ISP and associated NR-KPPs.

3) DoD Architecture Framework (DoDAF) (or Architecture) Products

The architecture products described in Table M-2 are minimally required to obtain an IATO for an Urgent UNS.

The SV-2, SV-6, SV-8 and TV-1 (2681) are presented in a single document that acts as the interim architectural products for the ISP. Submission of the PO-corrected 2681 to IA&JR fulfills the immediate architectural product requirement for an IATO.

PRODUCT	NAME	GENERAL DESCRIPTION
SV-2	Systems Communication Description	Systems nodes, systems, and system items, and their related communications lay downs.
SV-6	Systems Data Exchange Matrix	Provides details of system data elements being exchanged between systems and the attributes of that exchange.
SV-8	System Evolution Description	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.
TV-1	Technical Standards Profile	Listing of standards that apply to Systems View elements in a given architecture.

Table M-2: Urgent UNS-Required Architecture Products

Document template can be found on the C4II Knowledge Center Toolkit/Resources under the “ISP Information Support Plan Toolkit” folder. The PO will complete the template and associated system views, and provide the document to IA&JR for review. IA&JR will develop the draft TV-1, and provide it to the PO for review, modification and corrections. The PO will provide the corrected document, including SVs and TV, to IA&JR.

4) Plan of Action & Milestone (POA&M)

A POA&M is required to document the remaining tasks and timelines that the PO is agreeing to complete in exchange for an IATO from the Deputy Commander, C4I/I, allowing a rapid fielding of the Urgent UNS equipment. Minimally, this includes completion and approval of the SSAA, ISP and associated NR-KPPs, and receipt of JITC Interoperability Certification.

Document template can be found on the C4II Knowledge Center Toolkit/Resources under the “UUNS Universal Needs Statement Toolkit” folder. The PO will present the POA&M to IA&JR. Submission of the POA&M fulfills the immediate POA&M requirement for an IATO.

Prior to IATO expiration, the Program Office will have an approved, complete SSAA and other requirements to obtain JIC. Prior to ICTO expiration, the Program Office will have an approved ISP and associated NR-KPPs. These will replace the 2681 and are needed to obtain the required JIC. The assumption is that the Urgent UNS will be backfilled with a JCIDS capabilities document from MCCDC. It will be the responsibility of the PO to coordinate with MCCDC, AC PROG, and the SBT to determine the long-term plan for the Urgent UNS. The PO shall inform IA&JR once the direction is known to determine if remaining actions are still required.

M.2.2 Safety Release

The below information is compiled and provided to the Safety Office for review, with subsequent recommendation to the MDA.

Document template can be found on the Safety Knowledge Center under the Safety Risk Documentation folder, Safety Release and Safe and Ready Certification section. The PO must complete the form and provide it to the Command Safety Office, with a Safety Assessment Report for the equipment being fielded under the Urgent UNS.

M.2.3 DD-1494 Application for Equipment Frequency Allocation

An application for frequency allocation must be approved before funds are authorized for the development of any new equipment that will radiate electromagnetic energy, for equipment receiving RF if protection is desired. Frequency assignment in the appropriate frequency band must be obtained prior to the operation of any transmitting equipment for testing, training, or operational use. An approved DD Form 1494 is required before a frequency assignment will be granted.

Document template can be found on the Systems Engineering Knowledge Center, Spectrum Management folder, Spectrum Certification section. The PO must complete the form and provide it to the ACENG Spectrum Management Section prior to fielding the equipment under an Urgent UNS.

Table M-3 identifies the various points of contact for the documents required under this process. These names, email addresses and phone numbers were current as of the printing of this document, but may have changed.

DOC	SECTION	NAME	EMAIL	PHONE
SSAA IATC	IA&JR	CW03 Nancy Levesque	nancy.levesque@usmc.mil	703-432-3833
		Michael F. Davis	davismf@mcsc.usmc.mil	703-432-3824
ICTO	SE&I	Mike White	whitecm@mcsc.usmc.mil	703-432-3099
2681	IA&JR	Major Salmon	john.b.salmon@usmc.mil	703-432-3842
		Marty Marbach	marty.marbach@ngc.com	540-657-5128
		Michael F. Davis	davismf@mcsc.usmc.mil	703-432-3824
POA&M	IA&JR	CW03 Levesque	nancy.levesque@usmc.mil	703-432-3833
		Major Salmon	john.b.salmon@usmc.mil	703-432-3842
DD-1494	Spectrum Management, ACENG	GySgt Jeffreys	lavarra.jeffreys@usmc.mil	703-432-3791
Safety Release	Safety	Scott Rideout	scott.rideout@usmc.mil	703-432-3778

Table M-3: Points of Contact