

OCT 04 2002

MEMORANDUM OF AGREEMENT
BETWEEN
MARINE CORPS CHIEF INFORMATION OFFICER,
COMMANDING GENERAL, MARINE CORPS COMBAT DEVELOPMENT COMMAND,
AND
COMMANDING GENERAL, MARINE CORPS SYSTEMS COMMAND

SUBJECT: CHIEF INFORMATION OFFICER ROLES AND RESPONSIBILITIES

I. Background

The Marine Corps Chief Information Officer (CIO), Headquarters Marine Corps (HQMC), has the responsibility to provide strategic leadership of the Marine Corps information infrastructure and to interface with the Department of the Navy (DoN) CIO for Department Information Technology (IT) matters.

Marine Corps Systems Command (MARCORSYSCOM) has overall acquisition management responsibility for the Marine Corps.

The Marine Corps Combat Development Command (MCCDC) is responsible for the execution of the Marine Corps requirements determination process.

Because of the interrelationships between these organizations, and the overlap in the processes they support, there is not a definitive written statement of the roles and responsibilities of each. This lack of specificity has become more in focus recently in terms of responsibility for the confirmation of Clinger-Cohen Act (CCA) compliance, but is not limited to that function. Table 1 contains a list of items requiring clarification in terms of division of responsibility among Marine Corps CIO, MARCORSYSCOM and MCCDC.

II. Purpose

This Memorandum of Agreement defines a set of roles and responsibilities for MARCORSYSCOM, Marine Corps CIO, and MCCDC in terms of IT systems, including National Security Systems (NSS). This is intended to address only those functions defined in Table 1 and is not an all-inclusive compilation of the collective roles and responsibilities of these organizations. It is also not intended to preclude other organizations from having roles and responsibilities related to the functions listed but to synchronize the roles and responsibilities of MARCORSYSCOM, Marine Corps CIO and MCCDC in order to maximize the effectiveness of key IT organizations and ensure that the Marine Corps capitalizes on its IT investments. Each of the items in Table 1 below is amplified individually in section IV.

Table 1 - Responsibility Matrix

| | Responsibility | MARCORSYSCOM/DRPM | MC CIO/C4 | MCCDC |
|----|--------------------------------------|-------------------|--------------|-------|
| 1. | Clinger-Cohen Act | R, S | A* | S |
| 2. | DITSCAP (Application/System) | A | R, S | |
| | DITSCAP (Site Certification) | R, S | A | |
| 3. | C4ISP | A** | C | R, S |
| 4. | Manpower and Training Plan | A | R, S | R, S |
| 5. | Chief Integrating Architect | R, S | A | R, S |
| | Operational Architecture | R, S | R, S | A |
| | Systems Architecture | A | R, S | R, S |
| | Technical Architecture | A | R, S | R, S |
| 6. | Service Data Administrator | R, S | A | R, S |
| 7. | AIS/IT requirements validation | R, S | A | R, S |
| 8. | Enterprise Portfolio Manager | R, S | A | R, S |
| 9. | IT Capital Planning & Investments | R, S | A | R, S |

A - Approval Authority; R - Review; S - Support; C - Confirmation
(Service level approval)

* Approval means signing of the CCA confirmation letter

** PM develops, MARCORSYSCOM approval authority

III. References

- (a) Public Law 104-106 FY1996 Defense Authorization Act Clinger-Cohen Act of 1996
- (b) DoDI 5000.2, "Operation of the Defense Acquisition System"
- (c) SECNAVINST 5000.2C (draft), "Implementation of Mandatory Procedures for Major and Non-major Defense Acquisition Programs and Major and Non-major Information Technology Acquisition Programs"
- (d) OSD memorandum "Clinger-Cohen Act Compliance Policy" of 8 Mar 02
- (e) DoDI 5200.40, "DoD Security Certification and Accreditation (C&A) Process"
- (f) U.S. Marine Corps Project Officer's Certification and Accreditation Handbook, Ver 3.0, Sep 2000
- (g) Marine Corps Order P5239.1, "Information Assurance (IA)", draft of 7 Jul 99

- (h) DoDR 5000.2, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs
- (i) MARCORSYSCOM C4ISP Guide of 22 Apr 02
- (j) MARCORSYSCOM Acquisition Policy Letter 3-01 of 20 Jul 01
- (k) SECNAVINST 5000.36, "Department of the Navy Data Management and Interoperability"
- (l) DON Data Management Interoperability (DMI) Implementation Planning Guide of Mar 02
- (m) CJCSI 3170.01, "Requirements Generation System"
- (n) U.S. Marine Corps ORD Development Process Handbook
- (o) DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation (C&A) Guide, April 2001
- (p) National Security Agency (NSA)/Central Security Service (CSS) Information System Certification and Accreditation Process Guide (NISCAP)
- (q) Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within Information Systems, 5 Jun 99
- (r) Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JD-CSISSS), 31 Mar 2001
- (s) DoDI 5000.2 (draft) Operation of the Defense Acquisition System, 18 Jun 2002
- (t) DoDD 8000.1 (draft) Management of Department of Defense Information Resources and Information Technology

IV. Roles and Responsibilities

1. The Clinger-Cohen Act (CCA), reference (a), was enacted to resolve some long-standing systematic problems associated with the oversight, acquisition, management and use of IT investments. Implementation instructions for compliance with CCA are contained in references (b), (c), (s) and (t). Reference (d) identifies more specific guidance with respect to appropriate evidence of compliance with CCA. The preponderance of CCA compliance artifacts exists in acquisition documentation, and hence the acquisition community is best suited to prepare the appropriate CCA compliance documentation. In concert with the above-mentioned instructions, and in keeping with the basic precept of CIO responsibility and accountability for an agency's information resource management activities, the roles and responsibilities for CCA confirmation are established as follows:

a. Marine Corps CIO shall:

- (1) Together with MARCORSYSCOM, confirm that the system is being developed in accordance with the CCA.
- (2) Serve as the focal point for the USMC input to OSD IT registry.
- (3) Provide authority for MARCORSYSCOM to input information directly into the OSD IT Registry.
- (4) Co-Sign the CCA Confirmation letter.

(5) Co-lead Integrated Product Teams (IPTs) established to confirm CCA compliance for USMC IT programs.

(6) Co-lead an IPT to formally establish the process, procedures and guidelines for CCA confirmation.

(7) Participate in the Marine Corps Program Decision Meeting (MCPDM) process to voice unresolved CCA, as well as other IT, related issues.

b. MCCDC shall:

(1) Include appropriate outcome-based performance measures in both Universal Needs Statements (UNS) and Operational Requirements Documents (ORD).

(2) Support the CCA confirmation process, as required.

c. MARCORSYSCOM shall:

(1) Together with MC CIO, confirm that the system is being developed in accordance with CCA.

(2) Establish and document an internal process to ensure CCA compliance for Abbreviated Acquisition Programs.

(3) Update MARCORSYSCOM information in the OSD IT registry.

(4) Provide CCA compliance and other IT related concerns via the Milestone Team Assessments/MCPDM process in support of milestone and other key program decision points.

(5) Co-sign the CCA Confirmation letter.

(6) Co-lead Integrated Product Teams (IPTs) established to confirm CCA compliance for USMC IT programs.

(7) Co-lead an IPT to formally establish the process, procedures and guidelines for CCA confirmation.

2. Department of Defense Information Technology Certification and Accreditation Process (DITSCAP) is the standard DoD approach for identifying information security requirements, providing security solutions and managing information system security activities. References (e), (f) and (g) further define the DITSCAP and provide implementation instructions. References (o), (p), (q) and (r) are specific implementations of the DITSCAP for Sensitive Compartmented Information (SCI) and Cryptologic systems. Although DITSCAP maps to any system life-cycle process, and its four phases are independent of the life-cycle strategy employed, there are clear links between the DITSCAP and acquisition processes. In addition, reference (h) levies acquisition management responsibility on the PM for information assurance per reference (e). However, because the process supports an

infrastructure orientation with a focus on system mission, environment, and architecture, Marine Corps CIO participation is required as well. A HQMC/MARCORSYSCOM co-lead is most appropriate.

a. Marine Corps CIO shall:

(1) Execute the duties as the Designated Approval Authority (DAA) for the Marine Corps Enterprise (MCEN).

(2) Provide MITNOC support of the DITSCAP relative to systems that connect to the MCEN, and its successor, Navy Marine Corps ntranet (NMCI).

(3) Implement and provide support to the DITSCAP as required by reference (f) and (g).

b. MCCDC shall:

(1) Include appropriate information assurance performance parameters in IT ORDs.

(2) Provide support to the DITSCAP as required by references (f) and (g).

c. MARCORSYSCOM shall:

(1) Execute the duties as the DAA for all systems or applications acquired or developed under that command, or as requested for other systems, and for all applications or systems for which they are the functional sponsor or advocate.

(2) Implement and provide support to the DITSCAP in accordance with references (e) and (f).

(3) Ensure appropriate DITSCAP considerations are addressed at all milestone and other program decision reviews.

3. Command, Control, Communications, Computers and Intelligence Support Plan (C4ISP) is an acquisition requirement for all systems that connect in any way to the communications and information infrastructure. This includes IT systems, including NSS and all infrastructure programs. C4ISP development and approval is governed by the overarching requirements identified in reference (h). As authorized under reference (h), the Marine Corps has developed additional supplemental guidance in reference (i). While MARCORSYSCOM, as the Marine Corps acquisition agent, is the lead for C4ISPs, the relationship of the issues it addresses to operational architectures requires Marine Corps CIO and MCCDC support.

a. Marine Corps CIO shall:

(1) Provide Service level confirmation for C4ISPs in accordance with references (h) and (i).

(2) Develop a Marine Corps Order for C4ISPs that is coordinated with MARCORSYSCOM and MCCDC.

(3) Provide support to the C4ISP review process in accordance with references (h) and (i) and the C4ISP MCO, when approved.

b. MCCDC shall:

(1) Provide support to the C4ISP review process in accordance with references (h) and (i) and the C4ISP MCO, when approved.

(2) Provide input to the HQMC developed C4ISP MCO.

c. MARCORSYSCOM shall:

(1) Develop and ensure coordination of C4ISPs in accordance with references (h) and (i) and the C4ISP MCO, when approved.

(2) Provide input to the HQMC developed C4ISP MCO.

(3) Submit C4ISPs to the Marine Corps CIO for confirmation in accordance with references (h) and (i).

4. Manpower and training requirements for new and modified systems are properly acknowledged and addressed under the acquisition management framework in accordance with accepted acquisition policy and directives. However, others outside the acquisition community are interested in the related manpower and training impacts associated with a program. Those who are assigned the responsibility to make force structure changes to address manpower impacts and those who create and deliver appropriate training for new and modified systems are obviously concerned. In addition, based on recent shortcomings related to manpower impacts that were recognized via reference (j), the CIO has an interest in ensuring appropriate handling of manpower and training matters.

a. Marine Corps CIO shall:

(1) Provide support to MARCORSYSCOM with respect to manpower and training requirements via the MCPDM process.

b. MCCDC shall:

(1) Provide support to MARCORSYSCOM with respect to manpower and training requirements via the MCPDM process and reference (h).

(2) Implement structure changes required as a result of new/modified systems fielding in accordance with established procedures.

c. MARCORSYSCOM shall:

(1) Address manpower and training requirements for MARCORSYSCOM managed programs in accordance with references (b), (c), and (h).

(2) Coordinate manpower and training requirements with external stakeholders in accordance with the MCPDM staffing process and reference (h).

(3) Provide documentation to the office of the CIO to demonstrate that manpower and training requirements have been satisfactorily addressed for programs within the acquisition process.

5. The Marine Corps Enterprise Information Technology Architecture (EITA) is a set of IT principles, standards, guidelines, and statements of direction intended to facilitate and promote the design and procurement of interoperable systems. While the overarching vision for the EITA is the responsibility of the Marine Corps CIO, expertise to implement the vision is resident at both MCCDC and MARCORSYSCOM.

a. Marine Corps CIO shall:

(1) Approve the EITA.

(2) Delegate to MARCORSYSCOM the responsibility for the resolution of conflicts between operational, system and technical views of the EITA.

(3) Define and issue IT standards and policies consistent with the Defense Information Infrastructure Common Operating Environment, DON information standards and guidelines, the Global Information Grid (GIG), Joint Systems Architecture, Joint Technical Architecture and other DoD and Joint mandates.

(4) Ensure appropriate architecture considerations are addressed in AIS/IT requirements documentation as required.

(5) Manage and Integrate the Marine Corps EITA into the DON architecture framework.

(6) Develop processes that make use of documented architecture to guide IT investments.

(7) Develop the Roadmap for enhancing and modernizing the EITA and injecting new technologies.

(8) Support MCCDC coordination of operational concepts and architectures.

(9) Participate in the collaborative engineering environment for the development and maintenance of the EITA.

b. MCCDC shall:

(1) Develop and maintain Marine Corps operational concepts and architectures in coordination with Marine Corps CIO.

(2) Ensure appropriate architecture considerations are addressed in AIS/IT requirements documentation as required.

(3) Participate in the collaborative engineering environment for the development and maintenance of the EITA.

c. MARCORSYSCOM shall:

(1) Develop and maintain Marine Corps systems and technical architectures in coordination with Marine Corps CIO.

(2) Create a collaborative engineering environment to develop

(3) and maintain the USMC EITA.

(4) Ensure all IT programs developed at MARCORSYSCOM are compliant with the USMC EITA.

(5) Lead the collaborative team with Marine Corps CIO and MCCDC participation for the resolution of conflicts between operational, system and technical views of the EITA.

6. Service Data Administrator is a person or group that ensures the utility of data used within an organization by defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical data base designs, and defining data security procedures. Data Administration is the responsibility for definition, organization, supervision, and protection of data within an enterprise or organization (NBS Special Pub 500-152). That function belongs to the organization that oversees the management of data across the enterprise and is responsible for central information planning and control. For the Marine Corps, that organization is Marine Corps (CIO). However, implementation of that data administration program must be supported by MARCORSYSCOM and MCCDC.

a. Marine Corps CIO shall:

(1) Establish a USMC Data Administration Program in accordance with references (k) and (l).

(2) Develop operational plans for making sustainable improvements to data quality and accessibility.

(3) Provide USMC policy and planning guidance for execution of USMC data management processes.

(4) Establish accountability for data protection and data quality.

(5) Ensure data quality and accessibility and USMC data

architecture-compliant standards are addressed in AIS/IT requirements documentation as required.

b. MCCDC shall:

(1) Ensure data quality thresholds, data accessibility and USMC data architecture-compliant standards and structures are adequately addressed in IT requirements documentation as required.

c. MARCORSYSCOM shall:

(1) Ensure programs comply with the USMC Data Administration Program and DoD and USMC established data architecture standards and structures.

(2) Implement data quality metrics to ensure AIS/IT system data products meet customer requirements.

(3) Ensure AIS/IT system data is protected as required.

7. The requirements generation process is governed by reference (m) for the Marine Corps. MCCDC is responsible for the execution of the requirements generation process in the role as user representative for the Marine Corps. Reference (c) further delineates roles and responsibilities related to the requirement generation process in terms of requirements documentation preparation. In addition, MCCDC is in the process of creating a Marine Corps Order (MCO) for the Expeditionary Force Development System (EFDS) that will further define the Marine Corps requirements generation process.

a. Marine Corps CIO shall:

(1) Review/comment on the MCCDC developed EFDS MCO.

(2) Validate requirements for AIS/IT programs against the enterprise structure.

(3) Participate in the development of requirements documents for AIS/IT programs in accordance with references (c), (m) and (n) and the EFDS MCO, when approved.

(4) Otherwise support the EFDS in accordance with the EFDS MCO, when approved.

b. MCCDC shall:

(1) Ensure adequate coverage of AIS/IT program requirements validation and development process in the EFDS Marine Corps Order, in coordination with Marine Corps CIO and MARCORSYSCOM.

(2) Generate requirements documents for AIS/IT programs in accordance with references (c), (m) and (n) and the EFDS MCO, when approved.

(3) Otherwise support the EFDS in accordance with the EFDS MCO, when approved.

(4) Be the focal point for operational concept development for Joint Concept Development and Experimentation (JCDE).

c. MARCORSSYSCOM shall:

(1) Ensure requirements for MARCORSSYSCOM managed programs are translated properly in accordance with references (c), (m) and (n) and this document.

(2) Review/comment on the MCCDC developed EFDS MCO.

(3) Participate in the development of requirements documents for AIS/IT programs in accordance with references (c), (m) and (n) and the EFDS MCO, when approved.

(4) Otherwise support the EFDS in accordance with the EFDS MCO, when approved.

8. Portfolio Managers can exist in the USMC at many levels depending on the scope of the portfolio and the degree of roll-up of lower level portfolios. The Enterprise Portfolio Manager is the ultimate Portfolio Manager and has the enterprise visibility for both the horizontal and vertical integration of portfolios. Within the Marine Corps, the CIO serves as the Enterprise Portfolio Manger, overseeing all IT portfolios.

a. Marine Corps CIO shall:

(1) Establish and implement a portfolio management process in accordance with the USMC IT Capital Planning Guide.

b. MCCDC shall:

(1) Support the portfolio management process in accordance with the USMC IT Capital Planning Guide.

c. MARCORSSYSCOM shall:

(1) Support the portfolio management process in accordance with the USMC IT Capital Planning Guide.

9. IT Capital Planning is the process designed to provide a framework for sound IT spending decisions. The IT Capital Planning process includes "selection" of IT investments for funding via the Planning, Programming, and Budgeting System (PPBS), "management" of those IT investments in accordance with acquisition management regulations, including references (b), (c) and (h), and "evaluation" of the IT investments after deployment for determining their organizational performance. Although IT Capital Planning is linked to pre-existing, institutionalized processes within the Marine Corps, it is the Marine Corps CIO who actively ensures that IT is well represented and

integrated within those processes. The Marine Corps CIO is the lead for this function, with support from MARCORSYSCOM and MCCDC via their current roles and responsibilities in the PPBS and acquisition management processes.

a. Marine Corps CIO shall:

(1) Establish and implement the USMC Capital Planning Process. Develop a USMC Capital Planning Guide in support of item (1) above.

(2) Coordinate the USMC Capital Planning Guide with key stakeholders, including MARCORSYSCOM and MCCDC prior to approval and release.

b. MCCDC shall:

(1) Provide input to the USMC IT Capital Planning Guide.

(2) Support the "select" phase of Capital Planning Process via established roles and responsibilities in the PPBS process and the USMC Capital Planning Guide.

(3) Support the "manage" phase of the Capital Planning Process via established acquisition management policy and directives and the USMC Capital Planning Guide.

(4) Support the "evaluate" phase of the Capital Planning Process as guided by the functional advocates and the USMC Capital Planning Guide.

c. MARCORSYSCOM shall:

(1) Provide input to the USMC IT Capital Planning Guide.

(2) Support the "select" phase of Capital Planning Process via established roles and responsibilities in the PPBS process and the USMC Capital Planning Guide.

(3) Lead the "manage" phase of the Capital Planning Process via established acquisition management policy and directives and the USMC Capital Planning Guide.

(4) Support the "evaluate" phase of the Capital Planning Process as guided by the functional advocates and the USMC Capital Planning Guide.

Table 2 - Acronym List

| | |
|--------------|--|
| ACAT | Acquisition Category |
| AIS | Automated Information System |
| C4ISP | Command, Control, Communications, Computers and Intelligence Support Plan |
| CA | Certification Authority |
| CCA | Clinger-Cohen Act |
| CIO | Chief Information Officer |
| DAA | Designated Approval Authority |
| DITSCAP | Department of Defense Information Technology Certification and Accreditation Process |
| DoD | Department of Defense |
| DoN | Department of the Navy |
| EFDS | Expeditionary Force Development System |
| EITA | Enterprise Information Technology Architecture |
| JCDE | Joint Concept Development and Experimentation |
| GIG | Global Information Grid |
| HQMC | Headquarters, Marine Corps |
| IT | Information Technology |
| MARCORSYSCOM | Marine Corps Systems Command |
| MCCDC | Marine Corps Combat Development Command |
| MCEN | Marine Corps Enterprise Network |
| MCO | Marine Corps Order |
| MCPDM | Marine Corps Program Decision Meeting |
| UNS | Universal Needs Statement |
| NMCI | Navy Marine Corps Intranet |
| NSS | National Security System |
| PPBS | Planning, Programming and Budgeting System |
| USMC | United States Marine Corps |

Table 3 - Key Definitions

| | |
|---|---|
| Information Technology | Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. |
| National Security System | <p>Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:</p> <ul style="list-style-type: none"> o Involves intelligence activities o Involves cryptologic activities related to national security o Involves command and control of military forces o Involves equipment that is an integral part of a weapon or weapons system; or o Is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). |
| Expeditionary Force Development System | The process by which the Marine Corps identifies and defines requirements. |
| Certification Authority | The CA, sometimes known as the Certifier, is the official responsible for evaluating the technical and non-technical security features of the information system. |
| Designated Approval Authority | The Designated Approving Authority, sometimes known as the accreditor, is the official with authority to formally assume responsibility for operating an information system at an acceptable level of risk. |
| Automated Information System | <p>An acquisition program that acquires Information Technology (IT) except IT that:</p> <ul style="list-style-type: none"> o Involves equipment that is an integral part of a weapon or weapons system; or o Is a tactical communication system |
| Planning, Programming, and Budgeting System | The cyclic process by which the Department of Defense allocates resources. It consists of three distinct, but interrelated phases: Planning, Programming and Budgeting. |
| Global Information Grid | The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. |