



UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

MCIEASTO 5400.5
G4/G6/G9
19 Jul 10

MARINE CORPS INSTALLATIONS EAST ORDER 5400.5

From: Commanding General
To: Distribution List

Subj: DESIGNATION OF MARINE CORPS INSTALLATIONS EAST (MCIEAST)
COMMAND INFORMATION OFFICER (CIO), ROLES AND
RESPONSIBILITIES

Ref: (a) MCO 5400.52, Department of the Navy Deputy Chief
Information Officer Marine Corps Roles and
Responsibilities
(b) 40 U.S.C. 113-117
(c) DOD Directive 8000.01, "Management of the Department
of Defense Information Enterprise," February 10, 2009
(d) SECNAVINST 5000.36A
(e) DON memo of 20 Oct 05, "Department of the Navy
Knowledge Management Strategy"
(f) MROCDM 45-2002 (NOTAL)
(g) SECNAVINST 5000.2D
(h) DOD Instruction 8115.02, "Information Technology
Portfolio Management Implementation," October 30,
2006
(i) SECNAVINST 5430.7P
(j) SECNAVINST 5210.8D
(k) DOD Instruction 5000.02, "Operation of the Defense
Acquisition System," December 8, 2008
(l) E-Government Act of 2002, Title III, "Information
Security," December 2002
(m) DOD Instruction 8510.01, "DOD Information Assurance
Certification and Accreditation Process (DIACAP),"
November 27, 2007
(n) DON Data Management and Interoperability, DON Data
Management Interoperability Implementation Planning
Guide (NOTAL)
(o) DOD 8320.02-G, "Guidance for Implementing Net-Centric
Data Sharing," April 12, 2006
(p) DOD Directive 7045.20, "Capability Portfolio
Management," September 25, 2008

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited.

- (q) MCO 3900.15B
- (r) DOD Memorandum, "DOD Net-Centric Data Strategy," May 9, 2003
- (s) National Security Agency/Central Security Service Information System Certification and Accreditation Process Guide (NOTAL)
- (t) SECNAVINST 5239.3A
- (u) DOD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001 (NOTAL)
- (v) Department of Defense Net-Centric Services Strategy, May 4, 2007
- (w) DOD Directive 5220.22, "National Industrial Security Program," December 1, 2006
- (x) CJCSI 6211.02C, "Defense Information System Network (DISN): Policy and Responsibilities," July 9, 2008
- (y) DOD Intelligence Information Systems Security Certification and Accreditation Guide, April 2001 (NOTAL)
- (z) IA Pub 5239-22, "IA Protected Distribution System (PDS) Publication," October 2003 (NOTAL)
- (aa) DOD Directive 8190.3, "Smart Card Technology," November 21, 2003
- (ab) HSPD 12, "Policies for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- (ac) MCO P5512.11C
- (ad) FIPS 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006
- (ae) DOD Memorandum of 5 Dec 06, "Capstone Concept of Operations for Department of Defense Biometrics" (NOTAL)
- (af) DOD Memorandum of 18 Aug 06, "Department of Defense (DOD) Guidance on Protecting Personally Identifiable Information (PII)"
- (ag) SECNAV M-5210.1
- (ah) CJCSI 3170.01F "Joint Capabilities Integration and Development System," May 1, 2007
- (ai) DOD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
- (aj) MCO 5271.1A
- (ak) MCO 11000.25

Encl: (1) Terms

1. Situation

a. To comply with reference (a), Marine Corps Installations East (MCIEAST) realigned the Assistant Chief of Staff (AC/S) G-6 to functionally meet changing requirements within the Information Resources Management (IRM) and Information Technology (IT) communities. Accordingly, the AC/S G-6 is appointed as the Command Information Officer (CIO), MCIEAST. In the absence of the AC/S G-6 (CIO) or as otherwise directed, the Deputy AC/S G-6 will execute duties of the CIO.

b. In accordance with references (a) through (ak), the CIO will oversee the effective use of IT and employment of information management resources across the eastern region to successfully meet the goals and objectives required for delivery of required capabilities. Reference (c) further defines IT as 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. The term IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

c. The CIO supports the alignment of business processes through implementation of a segmented architecture and IT planning procedures for the protection of mission critical and mission essential systems through strengthened cyber security management and technical controls. The CIO will serve as, or team with, command competency leaders to ensure core IRM/IT/Information Assurance (IA) workforce training, certification, education and management requirements are identified and supported and consistent with Marine Corps, and Department of the Navy (DON) direction.

d. The CIO will ensure command compliance with Department of Defense (DoD), DON, and USMC IM/IT directives, guidance, statutes, regulations and policy. Additionally, the CIO will provide technical, equipment, and hosting support for the command's IM efforts and will promote the effective and efficient design, and operation of command level IRM processes.

e. Per reference (d), Information Management (IM) is the planning, budgeting, manipulating, and controlling of

19 Jul 10

information throughout its life cycle. IM allows the Marine Corps to gather, share, and learn from information and is focused on providing the right information at the right time in an understandable and useable format to enable decision making. Knowledge Management (KM) is defined in reference (e) as the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance. This operational function, advocated by Marine Corps Combat Development Command (MCCDC), enables organizational learning to improve mission performance.

f. The Federal government, DoD, DON, and the Marine Corps are organized to provide CIO policy and guidance. The Director, C4/DDCIO (MC) is responsible for overseeing and guiding the development and operation of the Marine Corps cyber environment which will support effective execution of IM and KM. Accordingly, the CIO has been reorganized into the following divisions and branches to focus on specific task areas:

(1) Marine Air Ground Task Force Information Technology Support Center (MITSC). The MITSC mission is to provide regional IT services and information assurance. The MITSC is comprised of eight branches: Headquarters, Electronic Key Management System (EKMS), Network Operating Systems (NOS), Network Management (NetMan), Information Assurance (IA), Customer Service Center (CSC), Navy-Marine Corps Intranet (NMCI), and Marine Corps Network Operations Support Command (MCNOSC) Detachment. The division serves as the central point for all implemented and operational IT issues and services. It manages the server farm(s), the Network Control Centers (NOCs) and the CSC which provides Tier 1 - 3 support with the MCNOSC Det providing Tier 4 services.

(2) Communications Management Division. The Communications Management Division is divided into three branches: Headquarters, Wired Infrastructure, and Wireless Infrastructure. This division provides advocacy, oversight and policy to support the installations' planning, provisioning, installation, and maintenance of telecommunications infrastructure. Specific areas of support include: Base Telephone Infrastructure (BTI), Enterprise Land Mobile Radio (ELMR), Radio Frequency Spectrum Management, Maintenance Management and Wireless Systems Management, and Integration.

19 Jul 10

(3) Command Information Office. The Command Information Office is comprised of five branches: Headquarters, Systems Architecture and Engineering, IT Project Management/Process Improvement, Policy and Acquisition/Enterprise Architecture, and IT/IM/KM. This division serves as the IRM Center of Excellence for MCIEAST by providing functional area managers with IT/IM Services that enable systems engineering, integration, management, capital planning and IT acquisition, end-user support, and information sharing through an enterprise architecture representing a reliable framework of business systems and applications that align with MCIEAST, and Marine Corps strategies. The Command Information Office implements policy and guidance on issues regarding IRM, to include the alignment of IT investments to business priorities, and strategies established by the Commanding General, MCIEAST. The Command Information Office supports the effective use of information resources, and the alignment of business processes through implementation of enterprise architecture, and IT planning procedures in accordance with Marine Corps policy and guidance.

(4) East Coast Regional GEOFidelis Center (GEOFIEAST). "GEOFidelis" is the Marine Corps' Program of Record for Installation Geospatial Information and Services (IGI&S). The Director, GEOFIEAST, serves as the MCIEAST Geospatial Information Officer (GIO) and liaison to the HQMC GEOFidelis Program Management Office. In accordance with reference (ak), GEOFIEAST serves integrated, standardized, and centrally managed geospatial technologies, information, and services, and facilitates the sharing of authoritative geospatial data throughout the Marine Corps, DoD, and other Federal government agencies. GEOFIEAST provides regional and installation functional area managers with an integrated Geographic Information System (GIS) that enables operational planning, analysis, and decision support. GEOFIEAST promotes information sharing and visualization of a geographic common operational picture through an enterprise architecture representing a reliable framework of business systems, interactive mapping web services, authoritative databases, and geospatial applications that align with MCIEAST and Marine Corps strategies. As the Regional Office of Primary Responsibility for the Marine Corps GEOFidelis Program, GEOFIEAST provides program management oversight, policy and guidance on issues regarding geospatial information and services, and the alignment of geospatial data

collection initiatives and investments to business priorities and strategies. GEOFIEAST provides technical support to sustain all geospatial systems, authoritative geo-databases, interactive mapping web services, and web portals hosted, including Server/Systems Management, Incident/Problem Management, Change/Configuration Management, Data Management, Mapping and Analysis, and Service Level Management as related to the Marine Corps GEOFidelis Program.

2. Mission. The CIO will implement strategic guidance in support of MCIEAST to enable effective and efficient application, modernization, functional integration, acquisition, management and protection of all IT resources, to provide the most cost-effective IT services, while meeting all applicable mandates, orders, and directives.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The CIO will implement and provide strategic leadership to ensure Marine Corps IT infrastructure, policy and governance effectively and efficiently supports MCIEAST and our supported warfighting commands, along with the USMC business enterprise. To meet this challenge, the CIO will develop strategies and plans to integrate into a single, disciplined Marine Corps Enterprise Network (MCEN) that provides commanders and staffs the ability to conduct operations through shared, secure, and reliable environments. The CIO will meet mandated governance while operating in a highly cooperative environment with the MCEN/MCNOSC, DON CIO, other Services, and operational commanders. Meeting this vision will ensure IT standardization, security, economies through prudent capital planning, and most importantly, a substantial informational advantage over potential adversaries.

(2) Concept of Operations. In executing responsibilities outlined in this Order, in accordance with references (a) through (ak), the CIO will coordinate requirements and execution with organizations both internal and external to MCIEAST. To accomplish these responsibilities, the divisions within the CIO have been reorganized based on functional areas to better align resources to meet the mandates of Headquarters Marine Corps (HQMC), DON and DoD.

b. Subordinate Element Missions

(1) AC/S G-6 CIO shall:

(a) Serve as CIO for MCIEAST.

(b) Provide the strategic leadership and stewardship for regional IT assets. Responsibilities include:

1. Leadership/Management. Serve as principal focal point for IM/IT matters with U.S. Marine Corps Forces Command (MARFORCOM), subordinate installations of MCIEAST, II MEF, other Federal agencies, DoD, Joint Staff, Allies, DON, Marine Corps command elements, other military departments, academia, and industry.

a. Serve as MCIEAST senior authority for IT programs and committees. Develop IT management critical tasks and supporting skills and knowledge for MCIEAST personnel to achieve Marine Corps missions and goals.

b. As required, serve as a member of, and or provide input to, the Marine Corps IT Steering Group (ITSG), Operational Advisory Group (OAG), Installations Technology Working Group (ITWG) and other "ad hoc" panels in accordance with references (a) and (i). Evaluate and implement ITSG recommendations and decisions to include, but not limited to:

(1) Coordinating development and implementation of USMC IT policies, processes, procedures, and standards.

(2) Identifying IT investment opportunities for MCIEAST that would result in shared benefits or cost avoidance/savings.

(3) Conducting the IT capital planning and investment process in accordance with established procedures and policy set forth by HQMC. Conduct value and risk assessments for internally developed IT initiatives and submit results to use in the Program Objective Memorandum (POM) Development Process.

c. Use a portfolio management approach to consider whether to continue, modify or terminate a program or project. Provide guidance and recommendations to Milestone Decision Authorities, Advocates, and other organizations.

2. Policy/Organization

a. Provide policy and guidance on MCIEAST IT systems and networks.

b. Provide policy and guidance for disaster recovery and continuity of operations plans (COOP) support requirements for regional IT garrison and tactical support systems.

c. Support HQMC, DON IT governance initiatives and the development of IT governance processes in accordance with reference (a).

d. Advise the DON Deputy CIO (MC) (DDCIO (MC)), via MARFORCOM G-6, on MCIEAST IT matters in support of the development of IT policy, strategic direction, guidance, and standards, in accordance with references (a) and (i).

e. Provide support and oversight to ensure interoperability of MCIEAST IT systems with DoD, DON, Joint, Federal, Allied, and Coalition systems.

f. As directed, participate with DDCIO (MC) in the development of the USMC/DON IM/IT Strategic Plan.

g. Ensure MCIEAST IT systems, applications and data are properly registered in the appropriate DoD/DON repositories and that such information is kept current in accordance with references (a) and (d).

h. Ensure full and accurate IT reporting is executed, in accordance with references (a) and (c).

3. Technology Management

a. Promote the application of proven advanced technology techniques, procedures and methodologies across MCIEAST.

b. Support established USMC/DON standards for IT interoperability.

19 Jul 10

c. Ensure that essential information services in support of MCIEAST COOP are available to alternate sites of MCIEAST subordinate commands and installations.

d. Support MCIEAST in the development and implementation of a DON IM/IT performance measurement program, which institutes Marine Corps IT accountability, and reports and monitors Marine Corps IT performance metrics.

4. Capital Planning

a. Serve as MCIEAST IT Portfolio Management Lead, overseeing all MCIEAST Functional Area IT Portfolios as they relate to the MCIEAST enterprise architecture constructs regarding mission areas, domains, and sub-portfolios.

b. Ensure compliance with DDCIO (MC) guidance that allows the implementation and maintenance of interoperable, cost effective and secure IT systems, applications, Marine Corps missions and goals.

c. Oversee the prioritization of IT investments, and projects within MCIEAST to maximize overall return on investment, and to set strategic vision goals and objectives for all Marine Corps IT programs.

d. Ensure IT applications are aligned with the thirteen Marine Corps designated functional areas, and the six Secretary of the Navy (SecNav) functional areas to provide a means to categorize, understand, and manage Marine Corps programs of record (i.e., systems), and software applications in accordance with reference (d).

e. Provide recommendations for prioritization of IT investments to the appropriate Marine Corps resource sponsor in accordance with reference (e).

5. Enterprise Architecture (EA)

a. Provide policy guidance for, and oversight of, MCIEAST EA efforts in accordance with references (a), (c), (j), and (u).

b. Plan, develop, maintain, and use the MCIEAST EA to maximize the business value of our investment in IT, and minimize the amount of unnecessary redundancy resulting

from disparate planning and development efforts related to information systems, applications, and IT which enable the warfighting and supporting establishment, in accordance with references (a), (c), (j), and (u).

c. Ensure MCIEAST EA efforts contribute to a single integrated naval component of the Global Information Grid (GIG) architecture, comply with DoD and DON policies and are aligned with Federal, DoD and DON reference models, in accordance with references (a), (c), (j), and (u).

d. Adhere to HQMC established IT standards and policies consistent with the Defense Information Infrastructure Common Operating Environment, DON information standards and guidelines, the GIG, Joint Systems Architecture, DoD IT Standards Registry (DISR), and other DoD and Joint mandates.

e. Determine and maintain final disposition of MCIEAST EA priorities and subsequent EA development, maintenance, and use efforts.

f. Ensure appropriate architecture considerations are addressed in Automated Information Systems (AIS)/IT requirements documentation and compliance with HQMC, and DON Net-Centric Data Strategy.

g. Integrate use of MCIEAST EA in IT capital planning and investment process.

h. Support Marine Corps efforts in the coordination of MCCDC operational views and Marine Corps Systems Command (MARCORSYSCOM) system and technical views.

i. Implement HQMC governance, policy and oversight of Marine Corps data strategy, data architecture and data management efforts in accordance with references (c), (e), (j), (s), (t), (u), and (v).

j. Govern the use of established data standards (e.g., metadata, authoritative data sources).

19 Jul 10

k. Govern the use of established information exchange standards (e.g., web services, universal core and common core, standard message formats).

l. Develop a roadmap for enhancing and modernizing the EA, and injecting new technologies.

m. Establish accountability for data stewardship, data quality, and accessibility.

n. Serve as MCIEAST approval authority over data management and information sharing planning, programming, budgeting, acquisition and governance.

6. Information Security/Information Assurance (IA). Serve as the MCIEAST Certified Approval Representative (CAR) in accordance with references (o), (x), and (y).

a. Review Marine Corps IT program IA strategies to assess and manage risk.

b. Execute Marine Corps IA responsibilities as assigned in the Federal Information Security Management Act (FISMA) and in governing DoD Directives in accordance with references (o) and (z).

c. As directed, submit input to HQMC/C4 for DON FISMA report.

d. Implement and support the Marine Corps IA Master Plan program in accordance with references (aa), (ab), and (ac).

e. Ensure MCIEAST IA program and plans are fully coordinated with HQMC/MCNOSC.

f. Integrate Marine Corps IA requirements with Marine Corps strategic and operational planning.

g. Identify information security requirements, provide security solutions, and manage information system security activities within the region in accordance with references (c), (q), (aa), and (ad).

19 Jul 10

h. Implement policy to facilitate strategic identity management initiatives throughout the Marine Corps, in accordance with references (ae), (af), (ag), (ah), (ai), (aj), and (ak).

i. Ensure MCIEAST subordinate commands formally establish IA managers (IAMS) within the S-6, that will have reporting relationship with the MCEN Designating Approving Authority (DAA), via the MCIEAST CAR in accordance with reference (a).

j. Ensure accountability for data protection in accordance with references (l) and (ag).

k. Implement tactics, techniques, and procedures (TTPs) developed by MCNOSC for IA personnel as required for computer network operations.

l. Implement policy to integrate computer emergency response (CER), IA, and CND provider activities into network operations (NETOPS), network management, and information dissemination.

7. IT Project/Program Management

a. Serve as validation and approval authority for MCIEAST IT requirements in accordance with references (c), (g), (h), (o), and (ah).

b. Provide technical advice and other assistance on IT issues to the Commanding General MCIEAST, his staff and subordinate installation commanders, in accordance with reference (a) and this Order.

c. Validate requirements for AIS/IT programs against the enterprise IT infrastructure in accordance with reference (a).

d. Participate in the development of requirements documentation for AIS/IT programs, in accordance with references (n), (t), (w), and (ah).

8. Spectrum Management

a. Serve as the approval authority for spectrum assignment and use within MCIEAST, in accordance with references (a) and (ai).

b. Define and evaluate the relationship between federal agency missions and spectrum management.

c. Assess the potential impacts on spectrum availability and management arising from increased domestic and international demand.

d. Identify and evaluate tools and techniques available for effective spectrum management.

e. Identify recognized sources of best practices in spectrum-efficient technologies.

f. Identify and resolve spectrum management architecture issues and interdependencies.

g. Develop and implement policy guidance for MCIEAST spectrum management.

9. Information Resources Strategy and Planning

a. Information Resource Management (IRM)

(1) Support and oversee development and compliance of USMC IM/IT Strategic Direction, guidance, statutes, regulations, and policy across the region, in accordance with references (a) and (k).

(2) Promote the effective and efficient design and operation of all major Information Resource Management processes in support of the region.

b. Knowledge Management (KM)

(1) Promote the effective use of technology to help information and knowledge emerge and flow to the right people at the right time to create value, in accordance with references (a) and (f).

19 Jul 10

(2) Identify, evaluate, and promote technologies that increase efficiencies in business processes.

(3) Promote the use of technology that contributes to the intellectual capital of MCIEAST.

(4) Implement Marine Corps-unique military and civilian IT training, and career management requirements.

(5) Provide support to the DDCIO (MC) in his role as the IT Workforce Leader. Ensure the core IT workforce training, certification, education, and management requirements are consistent with HQMC direction, in accordance with reference (a).

(6) Develop and implement a C4 human capital strategy for the region.

10. Process Improvement. Serve as the MCIEAST senior functional lead for IT continual process improvement initiatives within the Marine Corps.

11. e-Government

a. Promote infusing Marine Corps IT into government and governance processes.

b. Ensure support and oversee development and compliance with regulations posed by e-Government, boundary-spanning programs, and IT initiatives.

c. Provide oversight of e-Government to support interagency partnerships.

d. Identify, evaluate, and promote e-Government planning to strategic and operational IT planning, IT investment review, and enterprise architecture planning. Specifically, address e-Government through operational analysis of steady state investments and IT Review Board processes evaluating new investments or investments under development, as well as other means.

4. Administration and Logistics

a. Administrative and logistic support requirements previously established do not change as a result of this Order.

b. Supporting commands and organizations will fund travel required for their participation in required activities.

5. Command and Signal

a. Command. This Order is applicable to MCIEAST.

b. Signal. This Order is effective the date signed.



D. P. THOMAS
Chief of Staff

DISTRIBUTION: A

19 Jul 10

TERMS**Chief Technical Advisor (CTA)**

Under the direction of the DirC4/DDCIO(MC), the CTA provides essential support to the DirC4/DDCIO(MC) for the continuing assessment of ongoing IT acquisition and operations to determine their success in achieving Marine Corps IT objectives. The CTA also serves as the senior technical expert for all matters pertaining to the identification of IT requirements and leads the continuing assessment and identification of promising emerging C4 and information technologies for exploitation and application in the warfighting and business domains. The CTA provides executive level oversight and guidance in the development, focus, direction, implementation and use of the Marine Corps Enterprise Architecture and Data Architecture.

Clinger-Cohen Act (CCA)

The Information Technology Management Reform Act legislation that was designed to improve the way the Federal Government acquires and manages information technology.

Command, Control, Communications and Computers (C4)

Integration of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations.

Continuity of Operations Plans (COOP)

A plan that details the essential functions of an agency that will be handled during any emergency or situation that may disrupt normal operations, leaving office facilities damaged or inaccessible.

Department of Defense Chief Information Officer (DoD CIO)

Provides leadership to meet the Net-Centric vision and ultimately delivers the critical enabling capabilities required by the National Defense Strategy against an evolving threat from both internal and external sources.

Designated Approval Authority (DAA)

The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Director of Intelligence (DIRINT)

DIRINT Marine Corps manages Marine Corps SCI domains in close coordination with the DirC4/DDCIO(MC) to ensure that the enterprise-level management of SCI domains is comparable to that of the General Service domains. This relationship between the DirC4/DDCIO(MC) and DIRINT recognizes that special measures are required for the protection/handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of these measures must be tailored to comply with separate and coordinated Director of National Intelligence directives and Intelligence Community.

Director of National Intelligence

Serves as the Head of the Intelligence Community (IC). Acts as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security.

Enterprise Architecture (EA)

The current and/or future structure and behavior of an organization's processes, information systems, personnel, and organizational sub-units, aligned with the organization's core goals and strategic direction.

Expeditionary Force Development System (EFDS)

A standardized methodology used to translate needs into fielded, integrated capabilities for the regional combatant command's operating forces and supporting establishments to identify capability gaps.

Federal Enterprise Architecture (FEA)

An initiative of OMB that aims to comply with the CCA and provides a common methodology for IT acquisition in the federal government.

Federal Information Security Management Act (FISMA)

A comprehensive framework to protect government information, operations, and assets against natural or human made threats.

Functional Area (FA)

A distinct group of system performance requirements which, together with all other such groupings, forms the next lower-level breakdown of the system on the basis of function.

19 Jul 10

Functional Area Manager (FAM)

The individual or designated agency responsible for the management and planning of all personnel and equipment within a specific functional discipline.

Information Assurance (IA)

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Management (IM)

The entire process of defining, evaluating, protecting, and distributing data within an organization.

Information Resources Management (IRM)

Techniques of managing information as a shared organizational resource. IRM includes identification of information sources, type, and value of information they provide and ways of classification valuation, processing, and storage of that information.

Information Technology (IT)

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 by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency which: 1) requires the use of such equipment, or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Information Technology Steering Group (ITSG)

The USMC enterprise level governance body ensuring all IT related initiatives are in the best interest of the USMC.

19 Jul 10

Knowledge Management (KM)

The systematic process of discovering, selecting, organizing, distilling, sharing, developing, and using information in a social domain context to improve warfighter effectiveness. KM is the operational function of integrating people and processes, empowered by technology, to facilitate the sharing of relevant information and expertise. This function enables organizational learning to improve mission performance. IM allows organizations to gather, share, and learn from information, and is focused on providing the right information at the right time in an understandable and useable format to enable decision making.

Marine Corps Combat Development Command (MCCDC)

Develops fully integrated Marine Corps warfighting capabilities; including doctrine, organization, training and education, materiel, leadership, personnel and facilities, to enable the Marine Corps to field combat-ready forces.

Marine Corps Requirements Oversight Council (MROC)

Serves as a senior Marine Corps leadership forum to advise and support the Commandant of the Marine Corps in the execution of the Marine Corps Title 10 responsibilities.

MROC Review Board (MRB)

Reviews topics, makes recommendations, and is a subordinate guiding body to the MROC.

MCSC Marine Corps Program Decision Meeting (MCPDM)

Structured, formal system acquisition reviews, evaluate program progress in relation to requirement objectives and specific technical criteria appropriate to each phase of the acquisition process.

National Security Systems (NSS)

Encompasses the longstanding statutory treatment of military and intelligence mission-related systems and classified systems.

Planning, Programming, Budgeting and Execution System (PPBES)

The system for justifying, acquiring, allocating, and tracking resources in support of Marine Corps missions.

Sensitive Compartmented Information

Classified information is secret information to which access is restricted by law or corporate rules to a particular hierarchical class of people.

System Views

A SV includes graphics of systems and interconnections and provides for, or in support of warfighting functions. It defines the physical connection, location and identification of key nodes, circuits, networks and warfighting platforms, and specifies system and component performance parameters.

Technical Views

A TV identifies services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.