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

MCIEAST-MCB CAMLEJO 5400.5
G-6
16 JUN 2014

MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE CAMP LEJEUNE ORDER 5400.5

From: Commanding General
To: Distribution List

Subj: DESIGNATION OF MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE CAMP LEJEUNE REGIONAL COMMAND INFORMATION OFFICER (CIO), ROLES AND RESPONSIBILITIES

Ref: (a) SECNAV Memo "Designation of the Department of the Navy Deputy Chief Information Officer (Navy) and the Department of the Navy Deputy Chief Information Officer (Marine Corps)," August 22, 2005
(b) MCO 5400.52
(c) MCO 5239.2A
(d) SECNAVINST 5430.7Q
(e) SECNAVINST 5000.36A
(f) DOD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(g) SECNAVINST 5210.8D
(h) MCO 5230.20
(i) SECNAVINST 5239.3A
(j) DoD Net-Centric Services Strategy of May 4, 2007
(k) DoD Memo, "DOD Net-Centric Data Strategy," March 2007
(l) CJCSI 6211.02D, "Defense Information System Network (DISN): Policy and Responsibilities," January 24, 2012
(m) DOD Instruction 8520.02, "Public Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
(n) FIPS 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," June 23, 2006
(o) HSPD 12, "Policies for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(p) MCO 5512.11D
(q) DoD Memo, "Department of Defense (DOD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
(r) MCO 11000.25A
(s) DOD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
(t) E-Government Act of 2002, Title III, "Information Security," December 2002
(u) DOD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
(v) SECNAVINST 5000.2E

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

(w) DOD Instruction 5220.22, "National Industrial Security Program," March 18, 2011
(x) DOD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013

Encl: (1) MCIEAST-MCB CAMLEJ G-6 Organization and Mission

1. Situation

a. Background. Enclosure (1) of reference (a) states, "Information Management (IM) and Information Technology (IT) are vital to the Department's (Department of the Navy) mission readiness and are key enablers to achieving the goals of network centric warfare, business transformation, and fulfilling the President's Management Agenda." To meet the challenges of optimizing IM and IT in the 21st century across the Department of Defense (DoD) enterprise, references (a) and (b) establish a functional reporting chain of Chief/CIOs.

b. General. The Department of the Navy (DON) CIO reports directly to the DoD CIO, and provides IM/IT strategic direction and policy for the Navy and Marine Corps. The role of DON Deputy CIO (Marine Corps) has been delegated as a dual-hat to the Director, Command, Control, Communications, and Computers (C4), who continues to report to the Commandant of the Marine Corps for all C4-related matters. As directed, every Major Subordinate Command in the Marine Corps is required to establish a CIO. The purpose of this Order is to appoint the Assistant Chief of Staff (AC/S), G-6 Department, Marine Corps Installations East-Marine Corps Base, Camp Lejeune (MCIEAST-MCB CAMLEJ) as the CIO, to oversee the management of IM/IT throughout MCIEAST-MCB CAMLEJ and aligned installations.

2. Cancellation. MCIEASTO 5400.5.

3. Mission. The MCIEAST-MCB CAMLEJ CIO will provide and implement strategic guidance in support of the region, and aligned with higher headquarters (HHQ) direction, to enable the effective and efficient application, modernization, functional integration, acquisition, management, and protection of all IT resources, and to provide the most cost-effective IT services while meeting all applicable mandates, orders, and directives.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The CIO will provide the regional leadership and stewardship of resources to ensure Marine Corps IT infrastructure, policy, and governance are implemented effectively and efficiently to sustain MCIEAST-MCB CAMLEJ installations and supported

warfighting commands. This includes meeting the challenges of deploying unified voice, video, and data capabilities across the Marine Corps Enterprise Network (MCEN), which provides commanders and staffs the ability to conduct operations through shared, secure, and reliable information environments, in support of MCEN unification and regionalization. The CIO will meet mandated governance while operating in a highly cooperative environment with Marine Corps Installations Command, Marine Corps Network Operations and Security Center (MCNOSC), Marine Corps Cyber Command (MARFORCYBER), Marine Corps Systems Command, and the Commandant of the Marine Corps (C4). Meeting this vision will ensure regional IM/IT standardization, security, and economies through prudent capital planning and most importantly, in support of reference (b), a substantial informational advantage over potential adversaries.

(2) Concept of Operations. As the appointed MCIEAST-MCB CAMLEJ CIO, the AC/S, G-6 will coordinate the development and execution of IM/IT/Information Resource Management (IRM) requirements with organizations both internal and external to MCIEAST-MCB CAMLEJ. In addition, the CIO will perform the technical oversight and regional reporting requirements in accordance with reference (b). These responsibilities will be realized by leveraging the existing G-6 organizational structure outlined in enclosure (1) and aligning resources to meet the mandates of Headquarters, U.S. Marine Corps (HQMC), DON, and the DoD.

b. Subordinate Element Missions

(1) MCIEAST-MCB CAMLEJ Subordinate Commanders shall: In accordance with enclosure (1) of reference (b), and upon release of this Order, designate a CIO for your Installation or Battalion to coordinate all CIO matters on your behalf with the MCIEAST-MCB CAMLEJ CIO. In addition, establish or reaffirm an Information Systems Security Manager within your S-6 that will have a reporting relationship with the MCEN Authorizing Official (AO) via the MCIEAST-MCB CAMLEJ Certifying Authority Representative (CAR), in accordance with references (b) and (c).

(2) AC/S, G-6 shall: In conjunction with your responsibilities as the AC/S, G-6, serve as the CIO, MCIEAST-MCB CAMLEJ. In the conduct of the CIO role, you will report directly to the HHQ CIO on my behalf as necessary. In your absence, the Deputy AC/S, G-6 will execute duties of the CIO as directed below. This responsibility may not be delegated any further without my express written consent. Provide the strategic leadership and stewardship for regional IT assets. Responsibilities include:

(a) Leadership/Management shall: Serve as principal focal point for Regional IM/IT matters with HHQ, subordinate installations of MCIEAST-MCB CAMLEJ, tenant commands, other Federal agencies, DoD,

Joint Staff, Allies, DON, Marine Corps command elements, other military departments, academia, and industry.

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

2. As required, provide input to the Marine Corps IT Steering Group, Operational Advisory Group, Installations Advisory Group, and other ad hoc panels, in accordance with references (b) and (d). Evaluate and implement their recommendations and decisions to include, but not limited to:

a. Coordinating development and implementation of U.S. Marine Corps (USMC) IM/IT policies, processes, procedures, and standards.

b. Identifying IM/IT investment opportunities for the region that would result in shared benefits or cost avoidance/savings.

c. Conducting the IM/IT capital planning and investments process in accordance with established procedures and policy set forth by HQMC.

d. Conducting value and risk assessments for internally developed IT initiatives and submit results for use in the Program Objective Memorandum Development Process.

(b) Policy/Organization shall:

1. Provide policy and guidance on MCIEAST-MCB CAMLEJ IT systems and networks, including Disaster Recovery (DR) and Continuity of Operations Plans (COOP) support requirements for regional IT garrison and tactical support systems.

2. In accordance with references (b) and (d), support HQMC and DON IM/IT governance initiatives and the development of IM/IT governance processes by advising on MCIEAST-MCB CAMLEJ IT matters in support of the development of IT policy, strategic direction, guidance, and standards; and, as directed, participate in the development of the IM/IT strategic plans, policies and guidance.

3. Ensure MCIEAST-MCB CAMLEJ IT systems, applications and data are properly registered in the DON Application and Database Management System (DADMS) and the appropriate DoD/DON repositories, and that such information is kept current, in accordance with references (b) and (e).

4. Ensure full and accurate IT reporting is executed in accordance with references (b) and (f).

(c) Technology Management shall:

1. Promote the application of proven advanced technology, techniques, procedures, and methodologies across the region.

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

3. Ensure that essential information services in support of MCIEAST-MCB CAMLEJ DR/COOP are available to alternate sites of MCIEAST-MCB CAMLEJ subordinate commands and installations.

4. Support MCIEAST-MCB CAMLEJ in the development and implementation of a regional IM/IT/IRM performance measurement program, which establishes, monitors and reports IM/IT/IRM performance metrics, and ensures IM/IT/IRM accountability, in accordance with HHQ policies and programs.

(d) Enterprise Architecture (EA) shall:

1. Provide policy guidance for, and oversight of, MCIEAST-MCB CAMLEJ EA efforts, in accordance with references (b), (f), and (g).

2. Plan, develop, maintain, and use the MCIEAST-MCB CAMLEJ EA to maximize the business value of our investment in IM/IT, and to minimize the amount of redundancy resulting from disparate planning and development efforts related to information systems, applications, and web services, in accordance with references (b), (f), and (g). Integrate use of MCIEAST-MCB CAMLEJ EA in the IT capital planning and investment process.

3. Ensure regional EA efforts contribute to a single integrated naval component of the Global Information Grid architecture, by complying with DoD, DON, and HQMC policies and aligning with Federal, DoD, and DON reference models, in accordance with references (b), (f), and (g).

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

5. Support Marine Corps efforts in the development of EA views, such as operational, system and technical views.

6. Implement HQMC governance, policy and oversight of Marine Corps data strategy, data architecture and data management efforts across the region, in accordance with references (f) through (j).

7. Serve as MCIEAST-MCB CAMLEJ approval authority over data management and information sharing, planning, programming, budgeting, acquisition, and governance.

(e) Cybersecurity shall:

1. Serve as the MCIEAST-MCB CAMLEJ CAR, in accordance with references (c), (k), and (l).

2. Review Marine Corps Cybersecurity strategies to assess and manage risk within MCIEAST-MCB CAMLEJ. Implement a risk management framework to reinforce the security architecture of the MCEN.

3. Execute Marine Corps Cybersecurity responsibilities as assigned in the Federal Information Security Management Act and in governing DoD, DON, and Marine Corps Directives, in accordance with reference (k) within the region.

4. Ensure the MCIEAST-MCB CAMLEJ Cybersecurity program and plans are fully coordinated with HHQ.

5. Integrate Marine Corps Cybersecurity requirements with strategic and operational planning across the region.

6. Identify information security requirements, provide security solutions, and manage information system security activities within the region, in accordance with references (f), (h), (m), and (n).

7. Implement policy to facilitate strategic identity management initiatives across the region, in accordance with references (m) and (o) through (s).

8. Ensure MCIEAST-MCB CAMLEJ installations formally establish an Information Security Systems Manager within the S-6 that will have a reporting relationship with the MCEN AO via the MCIEAST-MCB CAMLEJ CAR, in accordance with reference (b).

9. Ensure accountability for data protection, in accordance with references (c) and (t).

10. Implement Tactics, Techniques, and Procedures developed by MCNOSC for cybersecurity personnel as required for Computer Network Operations.

11. Implement policy to integrate Computer Emergency Response, Information Assurance, and Computer Network Defense activities seamlessly within information dissemination processes and network operations and management.

(f) IT Project/Program Management shall:

1. Serve as validation and approval authority for MCIEAST-MCB CAMLEJ IM/IT requirements, in accordance with references (b), (f), (k), (u), and (v).

2. Provide technical advice and other assistance on IM/IT issues to the Commanding General, MCIEAST-MCB CAMLEJ, his staff, and installation commanders, in accordance with reference (b) and this Order.

3. Validate requirements for AIS/IT programs against the enterprise IT infrastructure, in accordance with reference (b).

4. Participate in the development of requirements documentation for AIS/IT programs, in accordance with references (i), (w), and (x).

(g) Spectrum Management shall:

1. Serve throughout the region as the approval authority for spectrum assignment and use, in accordance with references (b) and (s).

2. Define and evaluate the relationship between Federal agency missions and Spectrum Management.

3. Identify and resolve Spectrum Management architecture issues and interdependencies.

4. Develop and implement policy guidance for regional Spectrum Management.

(h) Information Resources Strategy and Planning shall:

1. Support and oversee development and compliance of USMC IM/IT strategic direction, guidance, statutes, regulations, and policy across the region, in accordance with reference (b).

2. 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 reference (b).

3. Provide regional support to the Deputy DON CIO (Marine Corps) 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 (b).

(i) Process Improvement shall: Serve as the MCIEAST-MCB CAMLEJ senior functional lead for IM/IT Continuous Process Improvement initiatives within the Marine Corps.

(j) e-Government shall:

1. Ensure support and oversee development and compliance with regulations posed by e-Government to support interagency partnerships.

2. 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 or investments under development, as well as other means.

5. 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.

6. Command and Signal

a. Command. This Order is applicable to MCIEAST-MCB CAMLEJ subordinate commands.

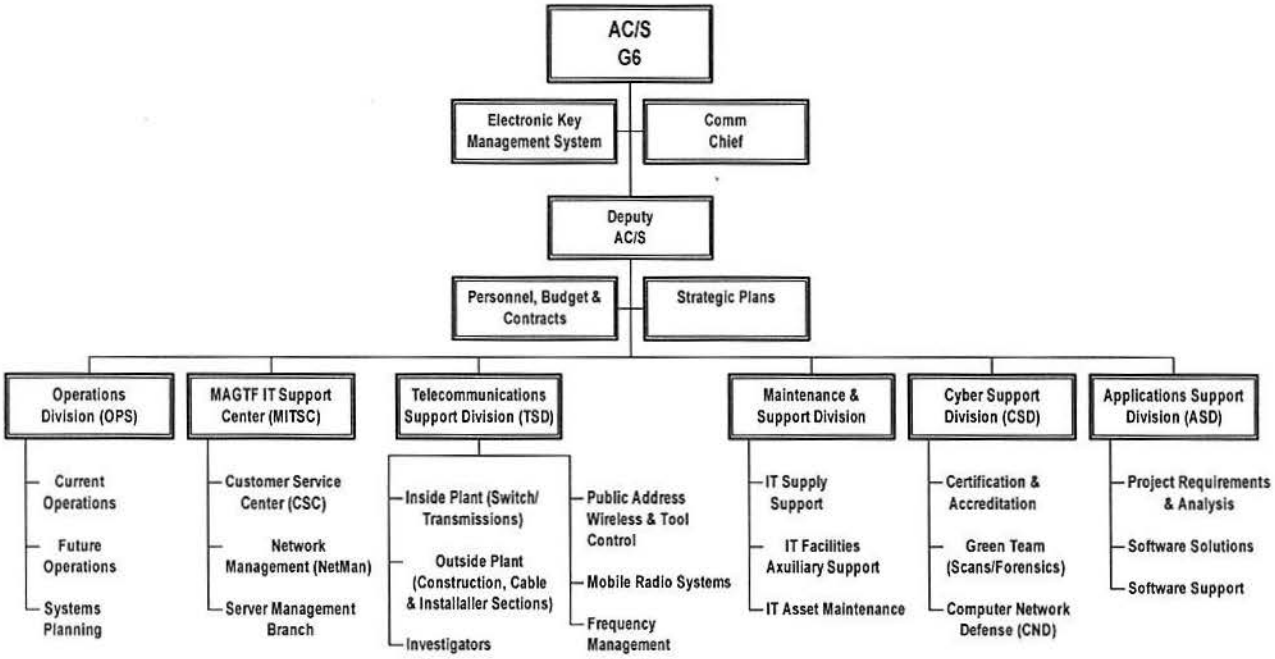
b. Signal. This Order is effective the date signed.

J. W. CLARK, JR.
Deputy Commander

DISTRIBUTION: A/B/C

MCIEAST-MCB CAMLEJ G-6 Organization and Mission

1. Organizational Chart



2. Mission. The AC/S, G-6 is the principal staff assistant on matters pertaining to IT Service Management. The primary mission of the MCIEAST-MCB CAMLEJ, G-6 is to plan, coordinate, and provide oversight of all Information Environments, Information Services, IT Infrastructures, and IT assets throughout the Region with a primary focus on Information Service support for the Operating Forces (OpFor) while in garrison. The G-6 provides the means for effective command and control (C2) of IT services, specifically in the areas of Marine Air-Ground Task Force Information Technology Center support, cyber security, IT asset management, encrypted communications, electronic equipment maintenance, and all IT infrastructure resident on each of the MCIEAST-MCB CAMLEJ installations, facilities, and training ranges.

3. G-6 Headquarters. The G-6 Headquarters is responsible for conducting all strategic planning in concert with HHQ policy and guidance, providing direct oversight of the Electronic Key Management System, establishing contracting requirements, monitoring contractor performance, developing budgets ordering supplies, and addressing all personnel and administrative matters.

4. Operations Division (OPS). OPS directly supports the AC/S, G-6 in managing regionally-controlled IT services, and executing the G-6 Regional IT Strategic Plan by achieving objectives through actionable

and measurable tasks in alignment with Marine Corps Information Enterprise Strategy. OPS conducts a wide range of Current and Future Operations planning to provide the means for effective C2 of both unclassified and classified enclaves operating on the MCEN. OPS plans and supports several transformative changes, including: (1) serving as the MCEN IT Center to ensure continuity of operations for Marine Corps Enterprise IT Services, and; (2) implementing the unification of MCEN military information services in accordance with the MCEN Unification Campaign Plan. Additionally, OPS is responsible for COOP/DR planning, Destructive Weather IT support planning, Service Level Agreement management, the Change Management process, Technical Writing, maintaining the G-6 document library, and department safety, environmental, and IT training matters.

5. Marine Air-Ground Task Force IT Support Center (MITSC). The MITSC provides 24/7/MCEN IT support to all Mid-Atlantic Region installations and tenant commands. This includes unclassified and classified IT services with primary focus on garrison networks, data hosting, COOP/DR and support for garrisoned OpFor. MITSC performs C2 Network Operations reporting to the MCNOSC and MARFORCYBER. The MITSC also: (1) maintains IT data centers for application/web/data hosting; (2) manages network transport for optimal connectivity; (3) manages network tools to defend and protect IT resources; (4) provides End-User Support via its 24/7/365 Customer Support Center, and; (5) manages data messaging, including official record message traffic and electronic mail.

6. Telecommunications Support Division (TSD). The TSD provides regional telecommunications support, enabling and managing access to a full range of telecommunications services for tenant commands, USMC, and Joint mission requirements, including: (1) official wire line and wireless voice services (BlackBerry, cellular telephone, air card) to MCB CAMLEJ, Marine Corps Air Station (MCAS), New River, and tenant commands; (2) telecommunications project management and quality control support for military construction and facility renovation projects in the region; (3) regional circuit management of all circuits, to include voice, video, data, security, special, and field training circuits; (4) commercial telecommunications training for OpFor personnel to enhance combat readiness; (5) public address system services to support special events aboard MCB CAMLEJ and MCAS New; River, (6) regional Spectrum Frequency Management to MCIEAST-MCB CAMLEJ agencies and coordination with Marine Expeditionary Force agencies, and; (7) Regional Land Mobile Radio/Enterprise Land Mobile Radio support.

7. Maintenance and Support Division (MSD). The MSD performs IT asset maintenance, which includes outfitting First Responder vehicles, repairing IT/radio assets, and performing 24/7/365 system restoration. MSD also provides IT facilities auxiliary support (data center and

telecommunication rooms), and reviews and processes local and regional IT procurement requests. MSD manages IT hardware and software assets, which includes supporting IT Service Requests for user accounts, asset moves, software installs, and network infrastructure projects; provides comprehensive asset lifecycle management by planning, acquiring, deploying, maintaining, and disposing of IT assets; and maintains break-fix inventory for service restoration.

8. Cyber Support Division (CSD). The CSD provides Cybersecurity program management to ensure authentication, confidentiality, availability, data integrity, and non-repudiation of messages and information exchange in support of C2 services in compliance with public laws, regulations, and policies. CSD oversees the Certification and Accreditation process for the Region. With guidance and support from MARFORCYBER, CSD uses defense-in-depth processes and capabilities, such as: (1) performing vulnerability scans and tracking compliance with Information Assurance Vulnerability Alerts/Bulletins and Operational Directives; (2) inspecting hardening of classified spaces; (3) responding to security events, identified vulnerabilities, and security risk directives, and; (4) conducting or supporting forensics investigations.

9. Applications Support Division (ASD). The ASD performs requirements analysis and provides subject matter expertise for development, deployment, and maintenance of new or existing automated information systems, and web services, including portals and web sites. ASD manages the IT Application Portfolio to track application ownership, configuration, investment and sustainment costs, reduce duplicative or redundant capabilities, and ensure proper system registration in the DADMS.