Marine Corps Enterprise Network (MCEN)
Secret Internet Protocol Router Network (SIPRNet)
Concept of Employment (COE)

MCEN SIPRNet – COE
Version 4.3

Headquarters United States Marine Corps (HQMC) Command, Control, Communications and Computers (C4)

Marine Corps Network Operations and Security Center (MCNOSC)

5 April 2010

DOCUMENT CHANGE RECORD

Version Number	Date	Description of Change
0.95	7/23/08	Initial Draft
0.98	1/15/09	Draft Release for Comments – S-5 NetOps Plans
0.99	1/21/09	Draft Release for Comments – S-5 Plans
1.0	3/6/09	Initial Draft Release
1.1	3/12/09	Initial Draft for HQMC C4 Comments
1.2	3/20/09	First Draft Release to HQMC C4
1.3	3/27/09	First Release for Staffing
1.4	6/10/09	Second Draft Release to HQMC C4
2.0	6/19/09	Second Release for Staffing
2.2	9/9/09	Second Release Working Copy – CRM Adjudication
2.41	9/11/09	Third Draft Release to HQMC C4
3.0	9/17/09	Third Release for Staffing
3.2	10/14/09	Working Copy – CRM Adjudication
4.0H	10/23/09	Fourth Draft Release to HQMC C4
4.0I	10/26/09	Minor update to Forward & Section 3
4.0J	02/02/10	Minor update to Section 2.6
4.1	02/28/10	Document renamed and added USCYBERCOM
4.2	03/12/10	Updated document based on Director C4 review
4.3	03/22/10	Updated document based on additional C4 leadership comments; Updated Appendix G (MarForPac)
4.3	04/05/10	Signed by Director C4

EXECUTIVE SUMMARY

This Concept of Employment (COE) describes the overall concepts, structures, and roles and responsibilities for NetOps Command and Control (C2), planning, Network Common Operational Picture (NetCOP), and systems management as it relates to the Marine Corps Enterprise Network's (MCEN's) Garrison Secret Internet Protocol (IP) Router Network (SIPRNet). It bridges strategic guidance and detailed operational procedures to describe how the MCEN Garrison SIPRNet is operated and defended through NetOps, much like the Tri-MEF SOP is to the tactical environment.

Concepts highlighted in this document are the Marine Corps regionalization strategy centered on four regions that form the backbone of all net-centric operations. The regions include National Capital Region (NCR), Atlantic, Pacific, and Reserves. Each region is supported by a Regional Network Operations and Security Center (RNOSC). The four regions encompass a total of eight sub-regions which are based on either geographical proximity or functional alignment. The sub-regions further support the regional backbone for all net-centric operations. All Marine Corps Bases/Stations (B/S) fall into one of these sub-regions. The sub-regions include Headquarters Marine Corps (HQMC), National Capital Region, East, Reserves, West, Mid Pacific, West Pacific, and Europe. Each sub-region is supported by a single Marine Air-Ground Task Force (MAGTF) Information Technology (IT) Support Center (MITSC) designed to provide IT services to garrison Marine Expeditionary Forces (MEFs) and Marine Corps Supporting Establishments (SE) within its area of responsibility. B/S provides touch labor in support of the MITSCs and Enterprise Service Desk (ESD).

Achieving operational control of the MCEN Garrison SIPRNet in this regionally-based architecture results in two significant changes to how commanders fulfill their NetOps missions.

- The first significant change is a realignment of NetOps authorities for global, regional, and local tasking and reporting. Operational NetOps reporting and execution is now accomplished through RNOSCs.

- The second significant change involves implementation of enterprise-wide Information Technology Service Management (ITSM) processes/tools for maintaining Situational Awareness (SA), network C2 in the execution of the NetOps mission, and delivery of IT services and capabilities to support garrison/deployed units. ITSM binds enterprise, regional, and local NetOps for the purpose of enabling warfighter C2 and providing effective, efficient, and responsive delivery of essential IT services to the Marine Corps customer and user bases. NetOps supports all aspects of the Marine Corps mission and spans all Marine Corps organizations. ITSM integrates the IT Governance, IT Acquisition, and IT Operations communities.

(Page intentionally left blank)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

FOREWORD

In 2008, C4 published the SIPRNet Transition Plan outlining the Marine Corps strategy to transition to Government Owned and Government Operated (GOGO) SIPRNet. This document takes the next step by laying out a conceptual framework for how the MCEN's Garrison SIPRNet will be planned, installed, operated, and maintained.

Concepts highlighted in this document build towards a resilient, cost-effective, enterprise network supporting the Commandant's regionalization strategy, which forms the backbone of all USMC net-centric operations. Key to our success will be a top-down, service-oriented commitment in delivering IT capabilities, instituting a new NetOps tasking and reporting framework, and clear delineation of the organizational roles and responsibilities spanning our IT governance, acquisition, and operational communities.

We will continue to refine and update this core document as our enterprise-wide Information Technology Service Management processes are implemented and the Secure Operational Network Infrastructure Communications (SONIC) Program of Record is established.

George J. Allen
Major General, U.S. Marine Corps
Director, Command, Control, Communications, and Computers (C4)

(This page intentionally left blank)

1. INTRODUCTION

The Secret Internet Protocol (IP) Router Network (SIPRNet) portion of the Marine Corps Enterprise Network (MCEN) is a subset of the Global SIPRNet which is a part of the Defense Information Systems Agency (DISA)-maintained Global Information Grid (GIG). The MCEN SIPRNet provides an efficient, effective, and protected network that enables situational awareness necessary for mission success, regardless of physical location. It provides the United States Marine Corps (USMC) with access to DoD's interoperable command and control data network, supporting collaborative planning, and numerous other classified warfighter applications. The MCEN SIPRNet spans both garrison[1] and tactical (deployed) networks. Figure 1 is a depiction of the end-to-end MCEN.

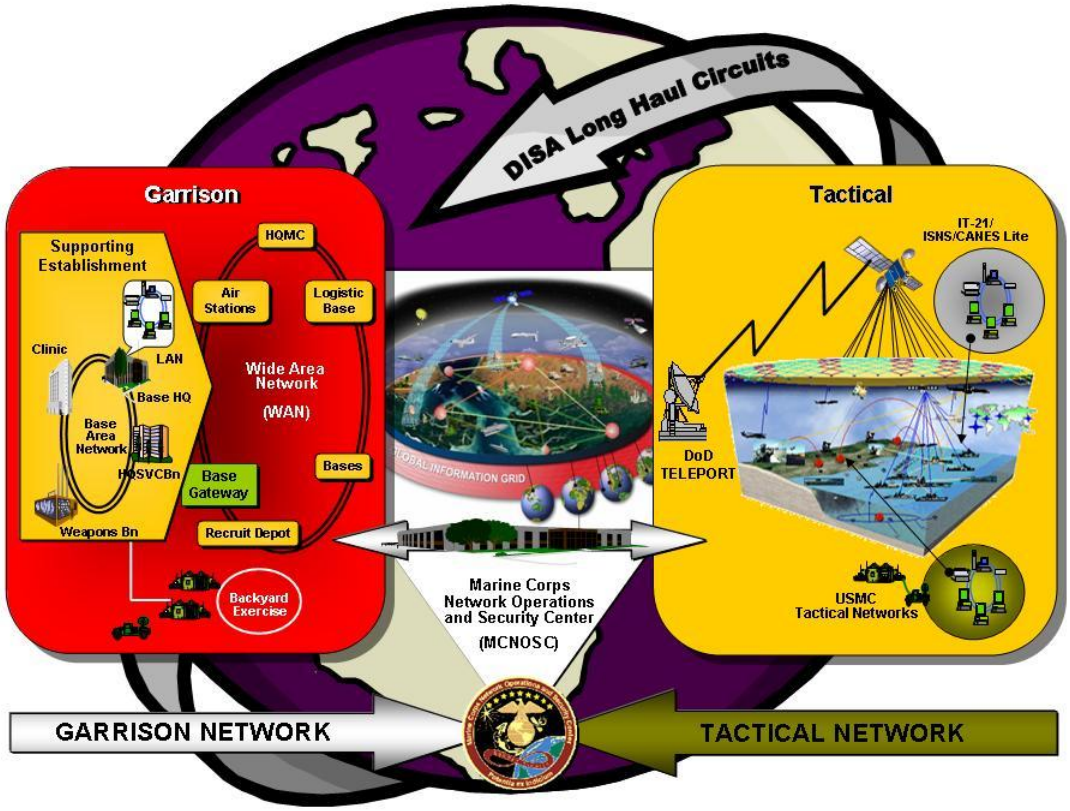

Figure 1: MCEN, Garrison to Tactical

The MCEN includes the Information Technology assets controlled and governed by the Marine Corps, either at an enterprise level or locally (such as deployed networks). The expansive reach of the MCEN touches and enables the entire gamut of USMC business and warfighting functions.

[1] Garrison is defined as a permanently-established facility or installation providing organic support to home-based USMC units. See section 2.7.3 for clarification of whether a unit is deployed or non deployed.

1.1. PURPOSE

The purpose of this document is to provide all Marine Corps stakeholders with conceptual information on how the MCEN Garrison SIPRNet is planned, installed, operated, and maintained. The COE will layout the road map for further development of IT Service Management processes and that will support operations.

This document is a reference for use by all Marine Corps SIPRNet stakeholders, but is specifically intended for the following audience:

- Defense Information System Agency (DISA)
- Marine Forces Cyber Command (MARFORCYBER)
- Headquarters Marine Corps (HQMC)
- Marine Corps Systems Command (MCSC)
- Marine Corps Network Operations and Security Center (MCNOSC)
- Regional Network Operations and Security Centers (RNOSCs)
- Marine Air-Ground Task Force (MAGTF) Information Technology (IT) Support Centers (MITSCs)
- Base, Station, and Component G6s
- Subordinate G6, S6, and Information System Coordinators (ISCs)
- Functional Area Managers (FAMs) and Functional Data Managers (FDMs)
- Program Managers (PMs) for IT Programs of Record (PoRs)
- MCEN Garrison SIPRNet users

1.2. RELATIONSHIP TO OTHER DOCUMENTS

This MCEN SIPRNet COE is a document in a series of Marine Corps Enterprise IT publications (refer to figure 2) designed to assist deployment and operation of capabilities into a fully integrated information technology environment compliant with DoD Guidance and Directives. In conjunction with the documents identified below, it contains necessary information for the deployment and operation of the Marine Corps SIPRNet.

Department of Defense Instruction (DoDI) 8410.02 instructs heads of the DoD Components to execute NetOps functions within DoD Component-operated portions of the GIG in accordance with Secretary of Defense Memorandum, "Assignment and Delegation Authority to Director, DISA," June 18, 2004 and in support of Combatant Commanders. This MCEN Garrison SIPRNet COE supports USMC execution of DODI 8410.02.

The COE also explains how to deliver regionalized MCEN Garrison SIPRNet NetOps conceptually by bridging the high level strategic view of the Marine Corps Integrated Communications Strategy (ICS), and low level (technical) information provided by Information Technology Instructions (ITIs).

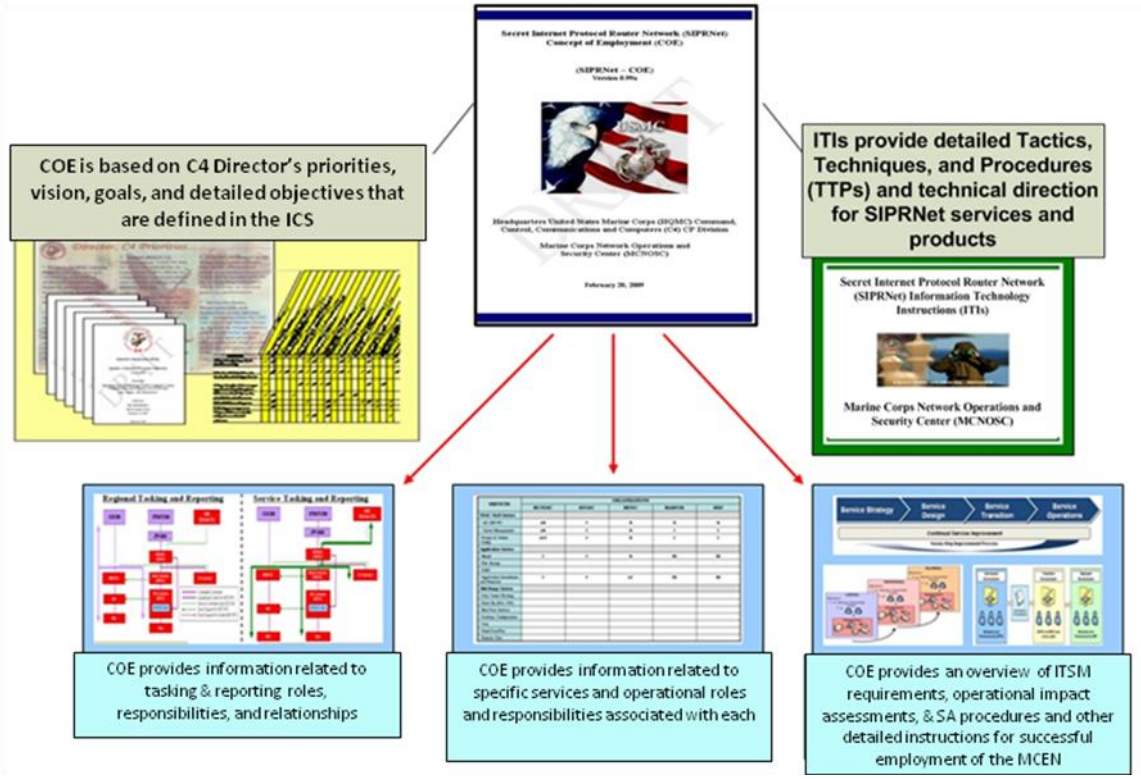

Figure 2: Document Relationship

1.2.1. Integrated Communications Strategy (ICS)

The ICS is a comprehensive vision, strategy, and planning document intended to unify and synchronize efforts of the Marine Corps IT community. The ICS encompasses the operating forces and the supporting establishment. Each appendix provides detailed planning information.

The primary focus of the ICS is to capture, document, aggregate, and integrate decisions that are made within various Marine Corps and Joint governance forums. The ICS contains the following seven appendices:

- Appendix A: Enterprise IT Concept of Operations (CONOPS)
- Appendix B: Network Strategy
- Appendix C: Service-Oriented Architecture, Information Access, & Web Strategy
- Appendix D: Applications Strategy
- Appendix E: Data Strategy
- Appendix F: Emerging Technologies Strategy
- Appendix G: Capability Development Roadmap (CDR)

The ICS Appendix A (Enterprise IT CONOPS) describes how the Marine Corps will shape MCEN operations and addresses the operational roles, responsibilities, and relationships between various Marine Corps Commands. The ICS Appendix A will be referenced throughout this MCEN SIPRNet COE, as it provides a description of the operational concept that the COE describes in greater detail.

1.2.2. MCEN SIPRNet Information Technology Instructions (ITIs)

ITIs are detailed Tactics, Techniques, and Procedures (TTPs) for the installation and implementation of various services and products. ITIs are currently being developed for all of the MCEN Garrison SIPRNet services and will be referenced throughout the document. In the future, these ITIs, services, and products will be documented and made available via shared portal, websites or collaboration tools. While the ITIs provide technical direction for configuring and operating specific aspects of MCEN Garrison SIPRNet infrastructure, the COE describes the operational and IT Service Management (ITSM) frameworks and specific organizational roles and responsibilities regarding the operations and maintenance of this infrastructure.

1.3. OPERATIONAL CONCEPT

Concepts highlighted in this document are built on the regionalization strategy centered on four regions that form the backbone of all net-centric operations. As shown in Figure 3, the regions include National Capital Region (NCR), Atlantic, Pacific, and Reserves. Each region is supported by a RNOSC. The four regions encompass a total of eight sub-regions which are based on either geographical proximity or functional alignment. The sub-regions further support the regional backbone for all net-centric operations. All Marine Corps Bases/Stations (B/S) fall into one of these sub-regions. The sub-regions include HQMC, NCR, East, Reserves, West, Mid Pacific, West Pacific, and Europe. Each sub-region is supported by a single MITSC designed to provide IT services to garrison Marine Expeditionary Forces (MEFs) and Marine Corps Supporting Establishments within its area of responsibility. Base and Stations (B/S) provide touch labor in support of the MITSCs and Enterprise Service Desk

Operationally, the MCNOSC functions as the NetOps[1] enterprise lead responsible for all cross-regional IT issues. The four RNOSCs provide NetOps oversight, approval authority, the tasking and reporting framework, decision support, and recommendations for MITSC(s) in their areas of responsibility. MITSCs execute NetOps functions for a sub-region in support of the RNOSC. Marine Corps B/S is responsible for providing technical support to the MITSCs. Approval authorities for NetOps reside with the G6 in support of the commander. Refer to Section 2.3 for more information.

[1] For more information on NetOps, refer to the Marine Corps ICS Version 2.5, Appendix A, "Enterprise IT Concept of Operations (CONOPS)"

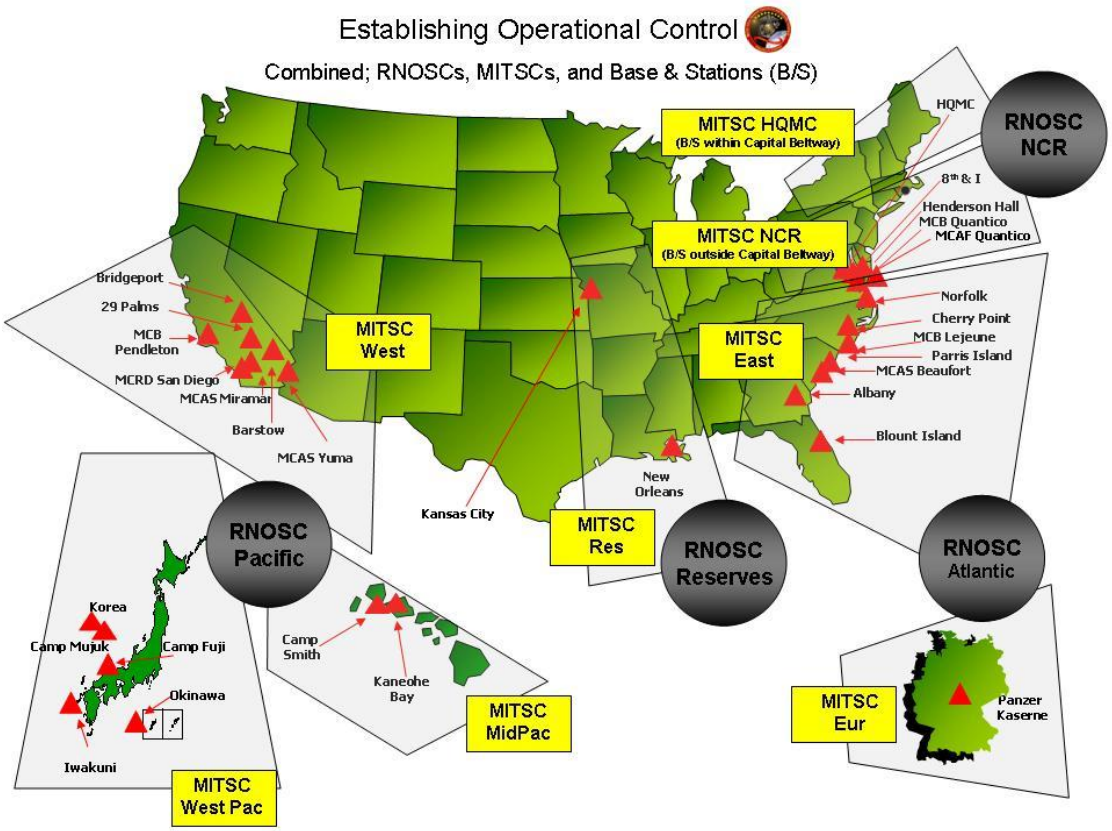

Figure 3: Enterprise Support, RNOSCs, MITSCs, and B/S Relationship

HQMC Director C4 provides governance, strategy, policy, and advocacy for the MCEN SIPRNet. MCSC will provide acquisition management for MCEN Garrison SIPRNet via the Secure Operational Network Infrastructure Communications (SONIC) Program of Record. MCNOSC as the operational arm of the MCEN in concert with the RNOSCs and MITSC will manage the day to day environment.

A key foundational component of the MCEN Garrison SIPRNet is the appropriate and consistent implementation of ITSM. ITSM enables delivery of IT services and capabilities to support the mission needs of MCEN Garrison SIPRNet customers.

1.3.1. NetOps Mission, Concept, and Tasks

NetOps is an operational construct used by the Commander, United States Strategic Command (USSTRATCOM) to operate and defend the DoD GIG. Joint NetOps encompasses activities associated with operating and defending networks, their applications, and their services. The objective of NetOps is to rapidly provide decision-makers with contextual information that allows them to make well-informed decisions that can quickly be passed to their forces for action. This is accomplished through the well-managed delivery of IT services, which requires shared situational awareness as well as the technologies, procedures, tools, and collaborative organizational structures to rapidly assess and respond to system and network degradations, outages, or changes in operational priorities.

NetOps mission essential tasks are GIG Enterprise Management (GEM), GIG Network Assurance (GNA), and GIG Content Management (GCM), with the enabling capabilities of Situational Awareness (SA) and C2. Figure 4 provides a graphic description of NetOps tasks and their effects[1].

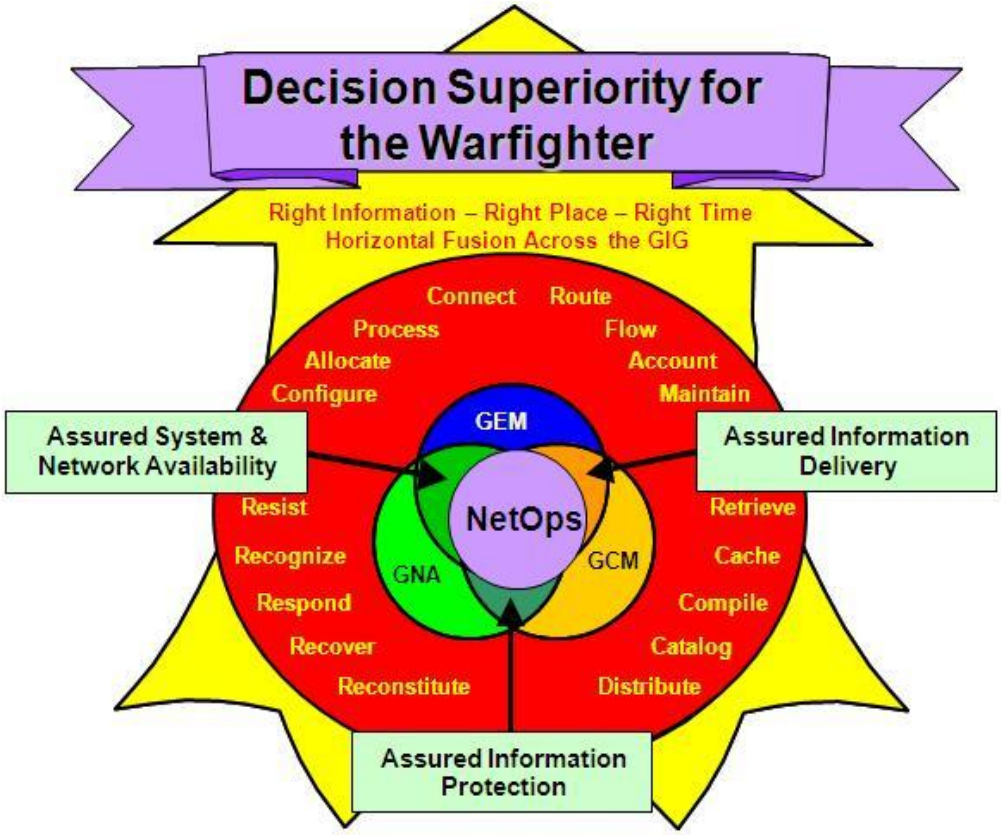

Figure 4: NetOps Essential Tasks and Effects

1.3.1.1. GIG Enterprise Management (GEM)

GEM includes the set NetOps functions encompassing the GIG's ITSM. These consist of the many elements and processes needed to communicate across the full spectrum of the GIG, to include enterprise services management, systems management, network management, satellite communications management, and electromagnetic spectrum management.

[1] The intent of this section is to provide only a general background on NetOps since it identifies the DoD-wide operational, organizational, and technical capabilities for operating and defending the DoD GIG. The MCEN is a subset of the larger GIG. Reference the DoDI 8410.02 for additional information and references.

1.3.1.2. GIG Network Assurance (GNA)

GNA includes the set NetOps functions that includes the operational responsibilities for information assurance, computer network defense (to include computer network defense response actions), and critical infrastructure protection in defense of the GIG.

1.3.1.3. GIG Content Management (GCM)

GCM includes the set NetOps functions that ensure information is available on the GIG by enabling users to safeguard, compile, catalog, discover cache, distribute, retrieve, and share data in a collaborative environment.

1.3.1.4. NetOps Situational Awareness (SA)

Situational Awareness, an enabling capability of NetOps, is achieving shared knowledge of the status of the network, its services, and its applications. Situational awareness improves the quality and timeliness of collaborative decision-making regarding the employment, protection, and defense of the network and, therefore, is a key enabler of C2. NetOps situational awareness is achieved by the following functions:

- **Visibility.** NetOps requires a real-time awareness of the "status" of its IT services infrastructure and security of the network.

- **Monitoring and Analysis.** NetOps requires the ability to receive status and performance related information about the resource(s) and provide discrete analysis, assess current or potential impact to warfighting and warfighting support missions, determine course of action alternatives, etc.

1.3.1.5. NetOps Command and Control (C2)

Given the nature of regionalized NetOps, many NetOps activities may not originate from a single command authority; therefore, C2 processes are needed to ensure unity of effort. The following NetOps C2 activities support the global integration of NetOps, across widely dispersed network operations centers, to operate and defend the network in a manner consistent with operational priorities and policies across the range of military and business operations. C2 will be covered in more detail in the next section.

- **Planning.** Planning establishes procedures and parameters for contingencies. It also establishes levels of operational control and delegated authorities for each organization involved in a specific operation or theater of action. Finally, planning evaluates current and past performance to gain lessons learned and to improve the planning process for future operations.
- **Coordinating/responding.** NetOps requires processes for quickly creating common action, movement, or condition among different elements to achieve the most effective results through unified and harmonious action. Coordination is inherent in command and can be one of the most important capabilities of a

commander employing the "centralized planning, decentralized execution" command style. Responding is the process of quickly reacting to stimulation and reacting appropriately to achieve the most effective results while preserving the integrity of the network.

- **Management.** NetOps requires the ability to make decisions concerning the installation, operation, and/or maintenance of available IT service infrastructure. It consists of those continuing actions of planning, organizing, directing, coordinating, controlling, and evaluating the use of personnel, money, materials, and facilities to accomplish missions and tasks.
- **Control.** NetOps requires the ability to direct and manage available resources, or allocate them to specific missions. The ability to exert control over these resources enables command functions, which are the ability to direct changes to resources as necessary to achieve a desired result within a specified timeframe.

1.3.2. IT Service Management (ITSM)

ITSM is an enabler of NetOps mission accomplishment. It supports the NetOps framework by providing effective, efficient, and responsive delivery of essential IT services to Marine Corps customers and users. In the future net-centric operational environment, the Marine Corps will become increasingly dependent on IT services and capabilities, so service management will become even more important.

ITSM is a framework of specialized functions and processes that, in conjunction with IT infrastructure and personnel, provides value to end users and customers in the form of IT services. ITSM processes support conceptualization, planning, procurement, implementation, and operation of IT services. Well defined process interfaces ensure the integration of acquisition, governance, and operational activities. Figure 5 shows the relationship between ITSM, IT Governance, IT Acquisition, and IT Operations.

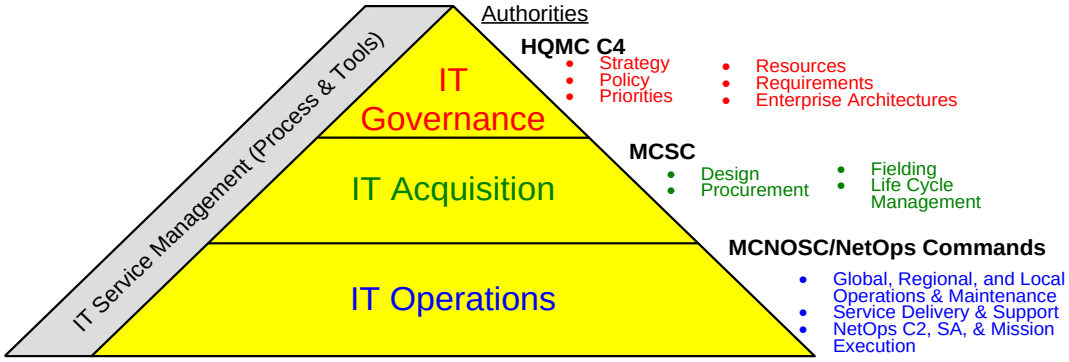

Figure 5: ITSM Process Correlation

Figure 5 also shows a general alignment of NetOps authorities and ITSM process correlations. These authorities include IT Governance, IT Acquisition, and IT Operations as defined in Appendix B. These three authorities map well, though not precisely, to the Information Technology Infrastructure Library (ITIL) v3 lifecycle and processes.

The ITIL framework provides a mechanism to bind organizations and statutory authorities performing governance, acquisition, and service operations within the Marine Corps. ITSM processes mutually support delivery of IT services and capabilities that exist within each NetOps authority. They integrate and span all authorities. With successful implementation of the ITSM framework, NetOps authorities can remain focused on the operational and/or functional needs of the customer and user bases through every process, resulting in not only more efficient services but services that are tightly integrated with the mission.

IT Governance helps to ensure all stakeholders, including senior Marine Corps leadership, internal customers, and in particular divisions such as finance or legal, have the necessary input into the decision making process. IT Governance is the steering function that provides overarching policies and directions for IT in support of the Marine Corps' overall mission and assures adherence to legal and regulatory requirements.

IT Acquisition is responsible for designing, developing, procuring IT service material solutions, and providing subsequent Lifecycle Management support, as appropriate for solutions and capabilities integrated into the fabric of the MCEN's Garrison SIPRNet.

IT Operations is responsible for delivering IT services and enabling value to the customer in terms of supporting mission accomplishment. IT Operations is supported by IT Acquisition through provision of resources. This, in turn, is supported by the organization's strategic assets in the form of goals and objectives.

ITSM, within the Marine Corps, is based upon the ITIL v3 framework which provides generic industry best practice guidelines and defines the following five lifecycle stages:

- **Service Strategy.** Provides guidance on how to design, develop, and implement IT services. Financial Management, Demand Management, and Service Portfolio Management (SPM) are among the primary processes comprising Service Strategy that are addressed in greater detail later in this document. These processes are foundational to supporting Marine Corps IT Governance.

- **Service Design.** Provides guidance and mechanisms for the design, development, and/or procurement of IT services. It covers design principles and methods for converting the strategic objectives of Service Strategy into catalogs of offered services. Service Catalog Management, Service Level Management, Capacity Management, Availability Management, IT Service Continuity Management, Information Security Management, and Supplier Management are the processes addressed in the Service Design section of this document.

- **Service Transition.** Provides guidance and mechanisms for justification and approval as well as subsequent transition for new services and/or enhancements to existing operational services. Change Management (ChM), Service Asset and Configuration Management (SACM) and Release and Deployment Management (RDM) are among the key Service Transition processes that are discussed in the Service Transition section of this document.

- **Service Operation.** Provides guidance on effective and efficient delivery and support of services to ensure value for the customer and user alike. Event Management, Incident Management, Service Desk, Problem Management, and Access Management are the critical Service Operations processes and functions discussed in the Service Operations section of this COE.

- **Continual Service Improvement.** Identifies and monitors processes so it can help correct problem areas within Service Strategy, Service Design, Service Transition, and Service Operation - with its proactive approach and keen sense of improvement on MCEN Garrison SIPRNet IT services.

Section 4 provides more detail on ITSM and the specific roles of IT Governance, IT Acquisition, and IT Operations organizations within the Marine Corps.

2. NETOPS TASKING AND REPORTING FRAMEWORK

2.1. THE MARINE CORPS NETOPS MISSION

NetOps within the Marine Corps is an operational, organizational, and technical construct for operating and defending the MCEN from the core to the tactical edge. The Marine Corps NetOps mission is to operate and defend the MCEN as a subset of the DoD GIG, as discussed earlier in section 1.3.1. Unlike many missions that are deemed successful at a defined completion date, the NetOps mission requires continual support to be successful. The following key functional areas are the Marine Corps equivalent to the three tenets of GIG NetOps previously discussed:[1]

- **MCEN Enterprise Management (MEM)** are the functional capabilities and operational processes necessary to monitor, manage, and control the availability, allocation, and performance within and across the MCEN. MEM includes enterprise services management, application management, systems management, network management, computing infrastructure management, satellite communications management, circuit management, and electromagnetic spectrum management.

- **MCEN Network Assurance (MNA)** is the set of functional capabilities and operational processes necessary to protect and defend the MCEN. These include computer network defense with associated response actions, critical infrastructure protection, and the operational management of IA capabilities. MNA activities consist of the policies and procedures that prepare systems, networks, and personnel to protect information.

- **MCEN Content Management (MCM)** is the set of functional capabilities and operational processes necessary to monitor, manage, and facilitate the visibility and accessibility of information within and across the MCEN. MCM maneuvers information across the enterprise, focusing on positioning and re-positioning of content to satisfy mission needs. MCM involves compiling, cataloging, caching, distributing, and retrieving data, managing information flow to users, and enabling the execution of the commander's information dissemination policy. MCM enables information users to define and set information needs (profiles) to facilitate timely information delivery, search information databases, and retrieve required products.

The effectiveness of NetOps within the Marine Corps will be measured in terms of availability, reliability, and security of Net-Centric services, across all domains, in adherence to agreed-upon service levels and policies.

[1] The intent of this section is to provide only a general background on MCEN NetOps. Reference the Marine Corps ICS Enterprise IT CONOPS [section 5.2] for more information and references.

The MCEN Garrison SIPRNet will be instrumented to allow the monitoring of adherence to standard Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) in use throughout the MCEN Garrison SIPRNet that define support to the warfighter. This instrumentation will enable timely NetOps decision-making, service prioritization, resource allocation, problem identification and resolution, and mission impact assessment. Future TTPs, service catalogs, and SLA/OLAs will be formalized with appropriate implementation policies, tools, and processes to ensure successful NetOps mission execution.

2.2. NETOPS COMMAND AND CONTROL (C2)

The Joint definition of command and control found in Joint Publication 1-02 is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Subsequently, Joint Pub 1-02 defines control as the authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations.

The Global SIPRNet enables command and control by supporting the achievement of information superiority, thus allowing commanders to make and implement better decisions faster than enemies can tolerate. This will put extraordinary demands on IT organizations associated with providing and overseeing the capabilities and services.

In the NetOps context, C2 provides direction for operations involving all garrisoned and deployed force systems on the MCEN SIPRNet. NetOps should not be confused with C2 of operations focused on other military missions. In an effort to safeguard the MCEN SIPRNet, streamline the NetOps process, and align NetOps execution to better support the warfighter, the Marine Corps is organizing NetOps around existing functional chains of command supported by NetOps organizations. The Marine Corps NetOps tasking and reporting framework is used to effectively balance centralized management (to facilitate rapid global execution) and decentralized management (for tailored and responsive support of regional and local IT services) to support all organizations that depend on the MCEN SIPRNet for effective mission execution. Commanders at all levels of the Marine Corps are responsible for effective control of their assigned portions of the MCEN SIPRNet. This requires close coordination within NetOps channels to achieve rapid, effective, and efficient execution of global, regional, and local directives.

2.2.1. Concept for Achieving Control of the SIPRNet

In order to gain effective control of the MCEN SIPRNet, it is necessary for commanders to succeed in executing the NetOps mission. Pre-requisites for effective control can be identified in five major areas. They include:

- Situational Awareness
- Unity of Effort
- Adequate ITSM Tools and Process
- Alignment of Services and Capabilities
- OLAs and SLAs

2.2.1.1. Situational Awareness (SA)

SA is needed by commanders at all levels to determine the impact of NetOps events on their missions and to direct necessary action to ensure mission success. This is especially true in the NetOps tasking and reporting framework for commanders charged with operating and defending the network under command of USSTRATCOM, USCYBERCOM, and geographic Combatant Commanders operating within their regions. Without adequate SA of the operational environment, effective NetOps control is not possible. Global SIPRNet capabilities must support building, maintaining, and sharing situational awareness at all levels to successfully operate and defend the network, including: real-time system and services status, threat and vulnerability status, and an understanding of on-going real-world operations and their linkage to critical data, applications, systems, and services. This can be done through automated reporting and data stores that provide real-time information that links IT services and capabilities to the specific personnel and organizations they support, those personnel/organizations to mission essential tasks directly affected, and those tasks to real-world military operations impacted. Effective operational SA also supports effective IT operations, acquisition, and governance. More on how the MCEN Garrison SIPRNet provides SA can be found in Section 3.

2.2.1.2. Unity of Effort

Unity of effort refers to the requirement to establish NetOps authority under an operational chain of command and to support those responsibilities with acquisition and governance authorities that are well understood and supported by effective processes for responsive decision making. Governance authorities provide policy and guidance to ensure standardization, support, and proper resourcing for emergent high priority requirements to ensure successful NetOps. Acquisition authority should ensure that IT contracts provide a legal basis for the NetOps commander to provide effective, detailed, and prioritized direction to vendor managed resources (infrastructure and personnel) in response to events on the network or the needs of supported commands and missions.

In a high operating tempo (OPTEMPO) environment where competition for resources is keen, such direction is necessary to ensure the best possible outcome to network outages and security events that impact supported commander mission requirements and/or USSTRATCOM directed actions. In order to achieve the proper alignment of authorities, attention to the careful structuring and segmentation of contracted services, performance-based supplier agreements that are enforceable and tie into SLAs between NetOps providers and warfighters, and vendor performance monitoring are required. Accommodation of surge or new service requirements within responsive well understood acquisition and governance processes is also necessary. Key decision makers must be aware of their responsibilities pending needs for approving or disapproving specific operations, acquisitions, requirements, funding or associated policies. Alignment of authorities and associated processes is discussed later in Section 4, describing service management roles and responsibilities.

2.2.1.3. ITSM Tools and Processes

The tools, services, and processes for executing command and control functions over the network must be adequate to ensure effective support to the warfighter. Standardized tools and processes are needed to rapidly assess operational impact of network events, facilitate planning, provide detailed direction, and to obtain and distribute timely and accurate reporting as operations develop. IT management structures, planning processes, tasking and reporting tools and procedures, trouble ticket management systems, and Network Common Operational Picture (NetCOP) tools must be carefully integrated. Local and regional commanders must have situational awareness of the GIG combined with access and authority for their respective Area of Responsibility (AOR) in order to effectively execute NetOps. This integration supports the decentralized execution and tailored support at the lowest level possible consistent with global standardization, integration, efficiency, and security. NetOps organizations must ensure next generation IT capabilities are include. A complete suite of robust tools and processes, appropriate to the increasing impact of NetOps on net-centric warfighting operations at all levels in the military chain of command, is necessary.

2.2.1.4. Alignment of Services

In order for NetOps functions to be responsive to the commands they support, capabilities and services must be aligned appropriately with military organizations and mission. The term “alignment of services” refers to the requirement to architect and manage services in a manner that allows for the direct and responsive support to warfighting and operational needs. For example, the “regionalization” of capability is a realignment of network capabilities and associated C2 to create more effective support to Marine Corps and Joint missions over a completely centralized model.

Alignment of services includes the architecting of Wide Area Network (WAN), directory services, server farm, security, service desk, and other infrastructures to support requirements of regional and local commanders that may be different. Such an alignment allows for the honing of services and responsive control of network resources necessary to both share and control access to mission critical data in response to unique mission requirements. To ensure effective operational control, responsiveness, adaptability, and survivability in support of the Department of Defense, Department of the Navy (DON) and supported Combatant Command (COCOM) operations, service and capability controls should be deployed to global, regional, and local levels in accordance with the nature of the particular service or capability. For example, day-to-day control of many network security capabilities may be global due to the nature of the threat and requirements to respond to USSTRATCOM direction, while access controls to the standardized shared data environment may be managed regionally and locally to ensure alignment and responsiveness to regional and local commands that own and use the data. Capabilities provided in the form of service will conform to SLAs between operators of the architecture and organizations they support. Additionally, redundancy, and failover capabilities that prevent or minimize large outages must be provisioned, and in the most extreme cases allow for a graceful degradation of outages by failing over control of critical services between global, regional, and sometimes local organizations. Considerations like these will significantly influence development and fielding of a robust and agile network environment that meets military requirements and is essential to supporting net-centric operations.

2.2.1.5. Operational Level Agreements (OLA) and Service Level Agreements (SLA)

Two mechanisms that are instrumental in supporting both the NetOps and customer communities in the effective delivery of IT services are the OLA and the SLA.

- OLAs are agreements between the Service Provider and other elements of the organization in support of the Service Provider's IT service delivery mission. They define the material and/or services that the supporting organization provides and the terms in which they provide them. In effect, these are the traditional Memorandum of Agreement (MOA) that the Marine Corps has long used but are specific to IT and placed in terms of the Service Level Management (SLM) process. As there are multiple service providing organizations, and none are self sufficient, OLAs become critical instruments for effective service delivery both within the regions and between the enterprise and regional NetOps layers.
- SLAs are agreements between the Service Provider and its customers. They cover details of the service(s) to be provided (a single SLA may cover multiple services or customers), document service level targets, and detail the responsibilities and commitments of both the Service Provider and customer. SLAs will be negotiated within the Service Level Management process.

2.3. NETOPS COMMAND RELATIONSHIPS

A NetOps tasking and reporting framework over the MCEN SIPRNet is necessary for NetOps to effectively support warfighting and warfighting support missions. However, before describing this organizational framework, it is necessary to understand command authorities and NetOps relationships. Command authorities and relationships are described in Joint doctrine. They include COCOM authority, Operational Control (OPCON), Tactical Control (TACON), and supported/supporting command relationships. They apply equally to execution of the NetOps mission and associated operations as they do to other types of missions and operations. It should be noted that these authorities are executed by commanders and describe relationships between commanders. They do not describe authorities and relationships between G6s. However, G6s execute NetOps under the authorities of their commanders utilizing NetOps capabilities and operations centers at their disposal.

2.3.1. Operational Control (OPCON)

The Joint definition of OPCON can be found in Joint Pub 0-2 and Appendix B. As applied to NetOps, OPCON involves TACON (section 2.3.2) authorities, plus:

- **Delineating NetOps functional/geographic responsibilities.** Establishing NetOps supporting relationships, shifting supporting responsibilities between network operations centers when operational forces transition within a region.

- **Assigning NetOps tasks and objectives.** Prioritizing response to network incidents or outages within a region.

2.3.2. Tactical Control (TACON)

The Joint definition of TACON can be found in Joint Pub 0-2 and Appendix B. As applied to NetOps, TACON involves:

- **Detailed NetOps direction.** Determining how apportioned resources are allocated, determining how changes to system configuration settings are implemented, implementing global information condition, setting local information condition as needed, etc.

- **Giving authoritative NetOps direction.** Directing how network and service resources are apportioned, mandating certain system configuration settings, establishing global information condition, etc.

- **Control of NetOps maneuvers.** Determining which systems need to be isolated in response to a network incident, providing users with network access, determining their level of access, allocating resources on the network, determining who can access their content, etc.

2.3.3. NetOps Supporting Relationships[1]

Joint Pub 0-2 describes several support relationships that are available for commanders to employ. A support relationship is established by the common senior commander of the commands under the support relationship. The different types of support relationship include: general, direct, and mutual. These Joint definitions can be found in Appendix B. By "regionalizing" or aligning IT capabilities of the Marine Corps with the operating forces and supporting establishment commands that are supported, direct support for these commands becomes possible.

[1] Reference USSTRATCOM, "Joint Concept of Operations for Global Information Grid NetOps" for clarification on NetOps C2 relationships.

Direct support is defined as, "A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance" (Unified Action Armed Forces (UNAAF) Joint Pub 0-2). Although other types of supported/supporting relationships are possible, the direct support relationship is used to define NetOps support between major commands in the Marine Corps. In order to clarify the direct support role of organizations in NetOps, the following framework is provided.

Limit of Direct Support Relationship

- Resources Allocated to Direct Support
- Availability of Direct Support
- Priority of the Direct Support Effort
- De-confliction

The support relationship can be described in both military and IT service management terms. At one level, Commands with NetOps responsibilities operate and defend the network on behalf of the commands they support. Supported commands require network dependant capabilities for their daily operations, which could include warfighting and warfighter functions. NetOps support relationships between major commands in the Marine Corps shall be standardized and made formal.

At another level, the support relationship is described in terms of IT service management. In these cases, specific OLAs and SLAs can be established and monitored. OLAs and SLAs will be standardized across all service support centers and IT organizations. In cases where a significant OLA or SLA is breached, Commanders' Critical Information Requirements (CCIR) may be triggered requiring notification. OLA and SLA use is especially important when commands require applications support or network services for applications they may manage internally. More on special support relationships for tenant commands, applications, and deploying units are found in Section 2.7.

2.3.4. Other Command Relationships

The two other command relationships used in this Concept of Employment are COCOM Authority and Administrative Control (ADCON). Complete Joint definitions are found in Appendix B.

2.3.4.1. COCOM Authority

COCOM Authority is defined in Joint Pub 1-02 as, "Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or Secretary of Defense.

COCOM Authority cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish missions assigned to the command." COCOM authority is normally exercised through the commanders of subordinate organizations, usually joint force commanders and Service and/or functional component commanders. COCOM provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions.

2.3.4.2. Administrative Control

Administrative Control is defined in JP 1-02 as, "Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations."

The Director C4 exercises ADCON over the MCNOSC. It includes the authorities necessary for the Marine Corps to install, operate, and maintain the MCEN SIPRNet as part of its Title 10 man, train, and equip responsibilities.

2.4. NETOPS AND SUPPORT ORGANIZATIONS

Multiple organizations are involved in execution of NetOps within the Marine Corps. The figure below provides a high level depiction of this with their SE relationships.

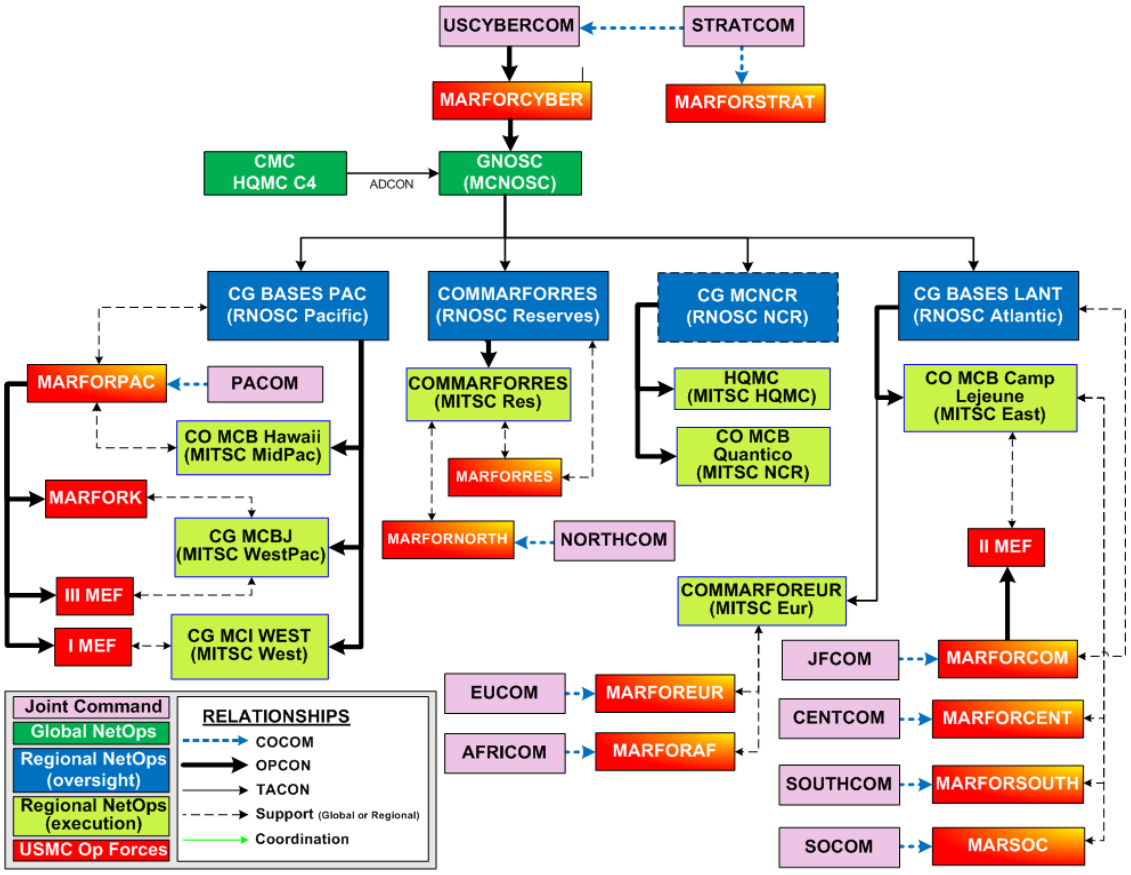

Figure 6: NetOps COCOM, MARFOR, and Supporting Establishment Relationships

2.4.1. United States Strategic Command (USSTRATCOM)

The Commander, USSTRATCOM serves as the DoD lead for NetOps. The USCYBERCOM serves as the NetOps execution arm of USSTRATCOM, which is responsible for planning, integrating, and coordinating DoD's global NetOps by directing GIG operations and defense and by identifying and advocating the desired NetOps characteristics and capabilities. Commander, United States Strategic Command (CDRUSSTRATCOM) exercises C2 through the USCYBERCOM. Successful operation and defense of the GIG requires an adaptive force comprised of professionals at the USCYBERCOM and throughout the NetOps community. The NetOps mission must be accomplished in support of Combatant Command mission priorities and in accordance with CDRUSSTRATCOM NetOps operational directives and guidance.

2.4.1.1. Marine Corps Forces, Strategic Command (MARFORSTRAT)

MARFORSTRAT serves as the service component to the USSTRATCOM. While not in the operational chain of command for NetOps, MARFORSTRAT does play a role in advocating USMC NetOps capabilities to USSTRATCOM on new capabilities requirement matters.

2.4.1.2. United States Cyber Command (USCYBERCOM)

USCYBERCOM is a subordinate command of USSTRATCOM that directs the operation and defense of the GIG across strategic, operational, and tactical boundaries in support of the DoD's full spectrum of warfighting, intelligence, and business operations. USCYBERCOM identifies and resolves computer security anomalies that affect the GIG's ability to support Office of the Secretary of Defense, Services, Joint Staff, supported combatant commands and the "warfighter."

The USCYBERCOM provides command and control of the GIG under the authority of the Commander, USSTRATCOM, through a tiered hierarchy of NetOps centers working together towards a common goal of assuring global decision superiority by maintaining near real-time situational awareness, end-to-end management, and dynamic DoD network defense. USCYBERCOM manages the GIG in accordance with the USSTRATCOM Joint Concept of Operations for GIG NetOps.

2.4.1.2.1. Marine Corps Forces, Cyber Command (MARFORCYBER)

MARFORCYBER serves as the service component to the USCYBERCOM. In this role, MARFORCYBER plans, coordinates, integrates, synchronizes and directs defensive cyberspace operations. MARFORCYBER is in the operational chain between USCYBERCOM and the MCNOSC.

2.4.2. Headquarters Marine Corps, Command, Control, Communications, and Computers (HQMC C4)

HQMC Director C4 provides strategy, policy, and advocacy for the MCEN SIPRNet. Through its role, HQMC C4 oversees the planning and delivery of IT capabilities that support both the warfighting and business domains of the Marine Corps. The C4 staff influences the combat-development process by establishing policies and standards for the Marine Corps enterprise architecture and fosters joint and combined interoperability. C4 manages governance processes and utilizes the Information Technology Steering Group (ITSG) and Operational Advisors Group (OAG) to support effective requirements prioritization and operational issues. HQMC C4, as resource sponsor and portfolio manager for IT capabilities, plays a key role in prioritizing requirements and IT implementation projects in the Marine Corps. Lastly, HQMC C4 has service command authority over MCNOSC for the purposes of executing Service Title 10 responsibilities over the MCEN SIPRNet.

2.4.2.1. Marine Corps Network Operations and Security Center (MCNOSC)

MCNOSC directs global network operations and network defense of the MCEN SIPRNet and provides technical leadership to facilitate seamless information exchange in support of Marine forces operating worldwide. MCNOSC is also responsible for intelligence gathering and analysis to develop future capabilities planning in accordance with NetOps CND. The MCNOSC operates under an OPCON relationship with USCYBERCOM/ MARFORCYBER to plan, execute, and/or direct the implementation of defensive measures to deter and defeat computer network attacks.

The MCNOSC is the Marine Corps' Global Network Operations and Security Center (GNOSC) responsible for the global operations and defense of the MCEN SIPRNet. MCNOSC operates the GNOSC for the Marine Corps and exerts global TACON over Marine Corps SIPRNet NetOps organizations. The MCNOSC has a C2 capability for executing global NetOps direction and can provide support to regional NetOps. It is designed specifically to support the Service. The MCNOSC is capable of building comprehensive SA at the global level and executing effective 24x7 NetOps C2 through its operations center, Watch Officer (WO), and watch standers. The MCNOSC is an integral part of the ITSM framework and is responsible for managing USMC Service Operations processes and supporting execution of Service Design and Service Transition processes. The MCNOSC provides global oversight and approval authority.

The MCNOSC is responsible for:

- **Shifting supporting missions when necessary.** The MCNOSC is responsible for re-assigning support missions. For example, the MCNOSC could re-assign supporting responsibilities when operational forces deploy from one region to another or in response to operational/network events.

- **Giving authoritative NetOps direction.** Directing how network and service resources are apportioned, mandating certain system configuration settings, establishing global information condition, etc.

- **Providing authoritative direction needed to coordinate global operations.** Certain management functions, such as security, need to occur on a global scale. The MCNOSC shall provide the authoritative direction needed for services that require global management.

- **Assigning tasks and objectives in response to global network events.** The MCNOSC shall establish priorities and assign tasks and objectives to subordinates based on USCYBERCOM global taskings.

- **Coordinating inter-regional operations.** Operations involving more than one region, such as execution of a Continuity of Operations Plan (COOP) between two RNOSC regions require global coordination and control by the MCNOSC.

The MCNOSC provides both System Control (SysCon) and Technical Control (TechCon) of the MCEN SIPRNet and interfaces with MARFORCYBER at the SIPRNet global level. MCNOSC TechCon manages MCEN enterprise capabilities that form core services is provided by MCNOSC Detachments that are located at each of the MITSCs described later in this section. While collocated, these Detachments are not part of the MITSC organization. Each Detachment reports directly to Commanding Officer MCNOSC and is responsible for owning and operating the Marine Corps enterprise managed assets/infrastructure that includes, but is not limited to: circuit infrastructure, directory services, e-mail services, NetCOP capabilities, and common Service Desk tools. The MCNOSC Detachment is available to support regional priorities when not managing global assets.

2.4.2.1.1. Enterprise IT Service Center (EITC)

The EITC is a data center designed to provide applications hosting and a standardized shared data environment. The EITC also provides portal services. Applications supported within the data center are global or "enterprise class" applications sponsored by the Functional Area Managers. The Marine Corps intends to deploy EITCs, under the operational control of the MCNOSC. The EITCs provide a critical part of MCM capability throughout the MCEN Garrison SIPRNet.

2.4.3. Marine Corps Force (MARFOR) G6

Marine Force (MARFOR) is the Marine component that provides operating forces, operation and contingency planning support, and advice to the respective combatant commander. The G-6 staff section is responsible for ensuring the MARFOR has the required communications and information systems in order to command and control Marine forces in support of the combatant commander.

All NetOps direction, tasking, and reporting for the region will be sent through the RNOSC, which is a function of the MARFOR G6 (For MARFORPAC and MARFORCOM the function is provided through their role as CG Bases PAC and CG Bases LANT respectively).

2.4.3.1. Regional Network Operations Security Center (RNOSC)

The RNOSC is an organization that provides regionally operated C2 capability for executing both regional and global NetOps direction. The RNOSC is capable of building comprehensive Situational Awareness at the regional level and executing effective 24x7 NetOps C2 through its operations center, WO, and watch standers. It provides regional oversight and decision support for approval authorities. It is free to operate within an assigned zone of action in accordance with service policy, standards, and TTPs. RNOSCs provide regional services as discussed in Section 5. They are focused on managing well-rounded regional NetOps (MEM, MNA, and MCM) tasks to include:

- Maintenance of NetOps situational awareness.
- Determination and execution of regional priorities/tasking.
- Conduct of regional operations impact assessments.
- Control of regional network defense response actions.

RNOSC(s) fall under the MCNOSC for global tasking and reporting. RNOSC(s) are TACON to the MCNOSC in executing of the USCYBERCOM NetOps direction. RNOSC responsibilities include.

- **Responding to direction and tasking from the MCNOSC.** The RNOSC ensures that global network operational directives from the MCNOSC are carried out.

- **Providing authoritative direction needed to coordinate regional operations.** The RNOSC shall provide the authoritative direction needed for regional management functions.

- **Assigning tasks and objectives in response to regional network events.** The RNOSC shall establish regional priorities and assign tasks and objectives to subordinates to accomplish them.

The RNOSC may delegate NetOps responsibilities to MITSCs to provide regional NetOps capabilities. The RNOSC relies on MITSCs to execute TechCon of IT capabilities operating within the region.

There are four RNOSCs that are located in the following locations:

- Marine Corps Base Quantico (RNOSC NCR)
- Camp Elmore (RNOSC Atlantic)
- Camp Smith (RNOSC Pacific)
- New Orleans (RNOSC Reserves)

2.4.4. Marine Corps Installation (MCI) G6

MCI is a part of the supporting establishment that furnishes support to the overall combat readiness of the Marine Corps. The MCI implements policies, develops regional strategies and plans, prioritizes resources, and provides services, direction and oversight through command of assigned USMC installations, in order to support the Operational Forces (OPFOR), tenant commands, and activities.

As a staff function within the MCI, the G-6 coordinates and supervises all NetOps functions of the supported Bases and tenant activities through the provisioning of a regional MITSC that is subordinate to the regional Base Commander, who also serves as the Commander of Marine Forces (COMMARFOR) and provides NetOps direction through a RNOSC.

2.4.4.1. MAGTF Information Technology Support Centers (MITSC)[1]

MITSC is a Marine Corps NetOps asset that is capable of executing direction within their assigned sub-region from the RNOSC. It is designed specifically to support MEF and major SE organizations and is generally owned by Marine Corps Installation (MCI) regional commands. The MITSC is capable of building comprehensive Situational Awareness at the sub-regional level and executing effective 24x7 NetOps C2 through its operations center, WO, and watch standers. It is focused on managing and executing NetOps (MEM, MNA, and MCM) functions under the C2 of the RNOSC and in support of commands at B/S within the sub-region. It supports all RNOSC C2/SA requirements, and executes its NetOps assigned missions. MITSCs provide regional services as discussed in Section 5 and HQMC message SIPRNET WAY AHEAD MITSC MSG 003-08/022047Z JUL 08/. A MITSC carries out MCEN Garrison SIPRNet service management functions that include:

- Incorporation of ITSM management tools and functions
- Execution of enterprise ITSM processes
- Execution of service-directed installation, upgrade, and maintenance on equipment and services
- Carry out directions for support by the Enterprise Service Desk (ESD)
- Verify and refine ITSM procedures and work instructions in the context of unique sub-regional requirements
- Manage access control for supported commands.
- Manage all regionally hosted services and applications.

[1] While MCNOSC Detachments are located at each of the MITSCs, they are not part of the MITSC organization. Each MCNOSC Detachment reports directly to Commanding Officer MCNOSC and is responsible for owning and operating Marine Corps enterprise managed assets/infrastructure.

There are eight regional MITSCs located at the following MCB and MCI locations:

- MCB Lejeune (MITSC East)
- MCB Pendleton (MITSC West)
- MCB Quantico (MITSC NCR)
- New Orleans (MITSC Res)
- MCB Butler (MITSC Westpac)
- MCB Hawaii (MITSC MidPac)
- Panzer Kaserne (MITSC Eur)
- Headquarters Marine Corps (MITSC HQMC)

2.4.5. Base and Station (B/S) G6/S6

It should be noted that local B/S G6/S6s receive NetOps direction and tasking from the MITSC within the established NetOps tasking and reporting framework discussed later in this document. The Marine Corps considers B/S networks (included in SE MD) as infrastructure to be managed under its Title 10 authorities. The G/S6s responsibilities including:

- Responding to direction and tasking from the MCNOSC, RNOSCs, and MITSCs. The local NetOps authority shall respond to tasking and direction from higher NetOps authorities, often constituting the local touch labor capability necessary for effective NetOps. In all but the most extreme of circumstances involving service outages or security incidents, direction to local NetOps authorities comes from the MITSC.
- Execution of enterprise ITSM processes.
- Verify and refine ITSM procedures and work instructions in the context of unique local requirements.

2.4.6. Tenant and Supporting G6/S6

Tenant and Supporting G6/S6 provide NetOps support to the regional MITSC as requested or directed.

2.4.6.1. Marine Expeditionary Force (MEF)

As the OPFOR, the MEF is the principle war fighting organization of the Marine Corps, organized to fight and win in conflicts up to, and including, a major war. While in a garrison environment, the MEF provides NetOps support to the regional MITSC as requested or directed.

2.4.6.2. Other Tenant Organization

Other tenant organizations provide NetOps support to the regional MITSC as requested or directed.

2.4.7. Marine Corps Systems Command (MCSC)

MCSC is the Marine Corps's principle agent for acquisition and sustainment of NetOps systems and equipment used by the operating forces to accomplish their warfighting mission. While involved in all ITSM lifecycle stages, its contribution to NetOps is primarily through Service Design, but MCSC is also instrumentally involved in Service Transition and Continuous Service Improvement (CSI).

2.4.7.1. Systems Integration Environment (SIE)

The SIE managed by MCSC provides a test and integration function for systems, applications, or services destined for or residing in the EITCs. This environment supports the engineering, design, Modeling and Simulation (M&S), integration, and deployment of technology-based solutions to maximize enterprise services performance and efficiency. The SIE is co-located with the Kansas City EITC. The capability, while routinely used to evaluate and support release of new capabilities into the MCEN Garrison SIPRNet, is available to support resolution of high priority incidents and problems that may arise within the MCEN Garrison SIPRNet.

2.4.7.2. Marine Corps Tactical Systems Support Activity (MCTSSA)

MCTSSA is the MAGTF Command, Control, Communications, Computers, and Intelligence (C4I) Systems Engineering Interoperability, Architecture, and Technology (SIAT) center for the Marine Corps. It is a component of MCSC that is located at Camp Pendleton, CA. MCTSSA plays a crucial role in the development, testing, implementation, and support of tactical applications. MCTSSA provides technical support, 24 hours a day, 7 days a week, and 365 days a year to deployed units - whether those deployments are for exercises or real operational requirements. Process interfaces between MCTSSA and the MCNOSC must be well-defined, because some tactical systems depend upon MCEN SIPRNet infrastructure and services. MCTSSA is part of the ITSM framework.

2.4.7.3. Secure Operational Network Infrastructure Communications (SONIC)

SONIC is a pre-decisional PoR that sustains and enhances many elements of the MCEN Garrison SIPRNet as a GO/GO network. SONIC supports implementation and sustainment of regional support and is ultimately responsible for Service Design and Service Transition lifecycle phases of the ITSM framework.

2.4.7.4. Other Programs of Record (PoRs)

Established PoRs provide organizational support for various capabilities in the MCEN SIPRNet. These programs enable information sources and services across the Marine Corps. They can also offer approaches that are market-based, enterprise-wide and tie into those that are Joint by design. PoR customers include the warfighter and support anyone within the Marine Corps community who needs specific services. PoRs are typically responsible for Service Design and Service Transition lifecycle phases.

2.5. USMC NETOPS TASKING AND REPORTING FRAMEWORK

2.5.1. Operational Environment and Command Relationships

In order to support the NetOps mission and to comply with requirements to support the needs of COCOMs and Marine Forces assigned to them, as well as those of the Service as a whole, including USMC SE commands and unassigned forces, the Marine Corps has realigned network infrastructures and services provided throughout USMC B/S. As identified in Figure 7, MCEN's SIPRNet infrastructure is divided into two types of Management Domains[1] (MDs) that are supported by physical network architectures and the necessary permissions and controls to operate them.

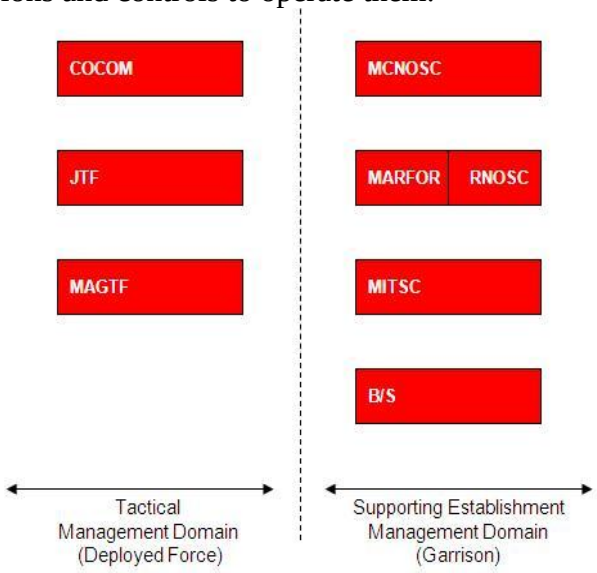

Figure 7: Depiction of NetOps Environment

[1] The term Management Domain (MD) should not be confused with an Active Directory (AD) domain. MD is used to describe a NetOps reporting structure, while an AD domain is part of a logical framework within AD.

The two types of MDs include:

1) A single SE MD, which is associated with the entire IT infrastructure within the B/S and non-deployable environment.

2) Tactical MDs associated with deployed networks inherent to the OPFOR. These Tactical MDs exist when forces (Marine Expeditionary Force (MEFs), Marine Expeditionary Unit (MEUs), and Marine Expeditionary Brigade (MEBs) deploy under the control of a COCOM, and when they exercise and operate in temporary tactical environments. While in garrison, services are provided through the MITSC as part of the garrison enclave within the SE MD. When deployed, IT services transition into the tactical MDs. NetOps tasking and reporting for this separate tactical enclave also changes. Transition processes and procedures are explained in Section 2.7.3.

Figure 8 depicts the command relationships between the commands responsible for operations. This figure also shows several of the operations centers that are part of the operational capability used by commands for executing NetOps, including the MCNOSC, the RNOSC, and the MITSC. Specific commands and support centers are described in the next section.

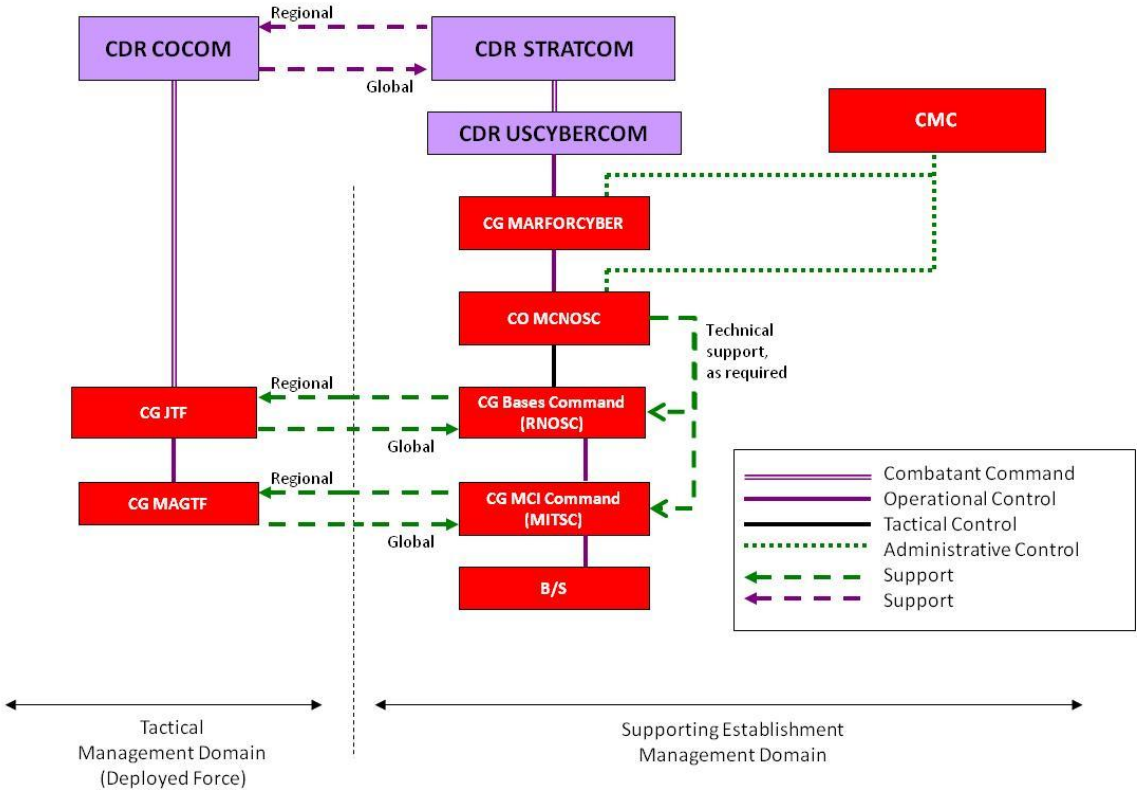

Figure 8: Depiction of Operational Environment and Command Relationships

The NetOps tasking and reporting framework is intended to mirror existing USMC chains of command to the maximum extent possible, leverage Commandant of the Marine Corps (CMC) directed regionalization of installations in 2005, and allow for effective use of RNOSC and MITSC operation centers for both globally and regionally directed NetOps. The designed IT architecture aligns with this framework, and, in most cases, existing chains of command. However, there are some cases where the physical locations of commands and bases as well as the need for effective IT architectures and C2 required structuring of the NetOps tasking and reporting framework that is not consistent with other reporting chains of command. In some cases completely new command relationships that did not previously exist have been created to ensure alignment under the four region/eight sub-region structure supported by RNOSCs and MITSCs.

A detailed reporting structure, listing nearly all USMC commands, units, or tenants can be found in Appendix G. The framework and associated RNOSC/MITSC structure depicted can be directly used for Marine Corps wide tasking and reporting initiated by either USSTRATCOM and USCYBERCOM or Headquarters Marine Corps. However, the framework is also structured in a way that allows USMC operating forces to use RNOSC/MITSC capabilities to support regional NetOps taskings from the Combatant Commanders.

2.6. NETOPS TASKING AND REPORTING

The GIG NetOps CONOPS describes three possible circumstances that determine the C2 of NetOps. They are known as global, theater, and non-global NetOps events. USSTRATCOM directs global events, respective COCOMs direct theater events, and the Services and DoD agencies direct their non-global events. For the purposes of this COE, non-global tasking and reporting will be referred to as Service tasking and reporting. The following sections describe the general rules for NetOps tasking and reporting within the MCEN Garrison SIPRNet, as well as specific considerations for global, regional, and Service tasking and reporting.

2.6.1. General Rules for Tasking and Reporting

In general, tasking and reporting is conducted in accordance with the framework shown in Figure 6 and Appendix G. Whether initiated by the Marine Corps Service Headquarters, USCYBERCOM, Geographic Combatant Commanders (GCC), or USMC Commanders, all types of operational tasking and reporting (global, regional, or service) are supported by the RNOSC/MITSC structure. The following general guidelines for tasking and reporting are provided:

- Tasking and reporting must be executed for all "exposed" assets on the network. This means that any asset connected to the network must comply with the mission task. Assets that are in storage need not be reported, but must however be brought into compliance prior to connection to the network. This is an important consideration since USMC network assets are often in transit. Non-exposed assets (that may at some point connect to the MCEN Garrison SIPRNet) must still be reported through the asset management database and life cycle management processes.

- Organizations that directly control assets on the network (e.g, have admin rights and exercise TechCon) are responsible for complying with NetOps mission tasks as well as routine maintenance and service support. NetOps organizations ensure that all assets on the network are visible and registered with the appropriate supporting MITSC. Individuals and organizations who directly manage the assets must be aware of their responsibilities with respect to reporting compliance for any taskings through the RNOSC/MITSC structure. Support contracts that involve technical control of assets by vendors must be written such that government visibility of asset status and reporting of compliance through the supported government organization is enforceable. It is the government's responsibility to ensure vendor compliance.

- Assets to include IT Program of Record systems connected directly to a MD are considered part of that MD and are reported through the chain of command associated with that MD. For example, tactical assets (laptops, etc.) connected to SE MD in garrison are reported through the SE chain of command, while all assets connected to a Tactical MD are reported through the chain of command associated with the operating force managing the domain.

- Procedures for transitioning assets from the one MD to another (e.g, SE to Tactical MD) must be standardized, closely controlled, and well understood. Examples include deploying assets from the garrison environment, conducting exercises in the field, or returning from the field and connecting tactical assets to the SE domain. Reference Section 2.7.3 for more details on transitioning assets.

- NetOps missions and mission tasks are issued via the established NetOps tasking and reporting framework as global and regional network Operational Directives (OpDirs). OpDirs are issued via record message traffic. The MCNOSC issues global OpDirs, while a RNOSC issues regional OpDirs. All OpDirs specify the directing authority (higher headquarters) and hence the originating chain of command. OpDirs use a standardized format and sequencing for tracking. Not all actions taken on the network are the result of an OpDir since there are many routine installation, maintenance, and security activities at any given time that may be directed through standard ITSM procedures. OpDirs generally result from a near term or immediate broad mission requirement, such as addressing an urgent security issue or an important operating force support requirement. They are often the result of DoD Communication Tasking Orders (CTOs), Information Assurance Vulnerability Alerts (IAVAs), USCYBERCOM Fragmentary Orders (FRAGOs), COCOM directives, or Information Condition (INFOCON) measures. NetOps authorities may also issue Operational Advisories (OpAdv) or Warning Orders (WARNORD) to notify the chain of command of a potentially hazardous situation or pending actions on the network. Standardized formats for OpDirs and OpAdv can be found in Appendix F.

Even though NetOps missions and mission tasks are issued via the established NetOps tasking and reporting framework, like other more routine activities on the network, they are accomplished through the disciplined application of standardized ITSM tools and processes. Execution is conducted with the support of the tools available to the NetOps centers (test environments, trouble ticket systems, NetCOP, configuration management databases, collaborative suites, etc.), and through the use of change management, configuration management, and other ITSM processes.

2.6.2. Global Tasking and Reporting

Global NetOps events are those activities that have the potential to impact the operational readiness of the Global SIPRNet and require a coordinated response from the entire NetOps community. Global tasking originates at the Joint level and includes Joint NetOps direction applicable to the entire DoD, including COCOMs and Services. Two clear tasking and reporting lines exist – one along the TMD and one along the SED. Additionally, situational awareness is provided from MARFOR to COCOM for garrison Marine Corps assets/compliancy within COCOM's theater of operations and from MAGTF to MARFOR for deployed Marine Corps assets/compliancy directly supporting the COCOM.

CDRUSSTRATCOM is the supported COCOM with all other Combatant Commanders/Services/Agencies (CC/S/As) in direct support. CC/S/As are responsible for leading the response to global NetOps events in accordance with USSTRATCOM and USCYBERCOM direction. USCYBERCOM Service NetOps components, including the MCNOSC, execute global NetOps missions and mission tasks.

Figure 9 depicts the general tasking and reporting for Global NetOps. The MCNOSC conducts mission analysis and planning with major subordinate NetOps organizations including those represented or directly supported by the four RNOSCs. OpDirs are only issued after careful consideration for implementation that may have a unique impact to the MCEN SIPRNet operating environment and supported USMC organizations and missions. The MCNOSC uses Operational Reporting Directives Reporting System (OPDRS) to automate and standardize the reporting process and to provide visibility of execution throughout the Marine Corps NetOps community. DoD reporting systems like the Vulnerability Management System (VMS) are also used where required (typically within the TMD).

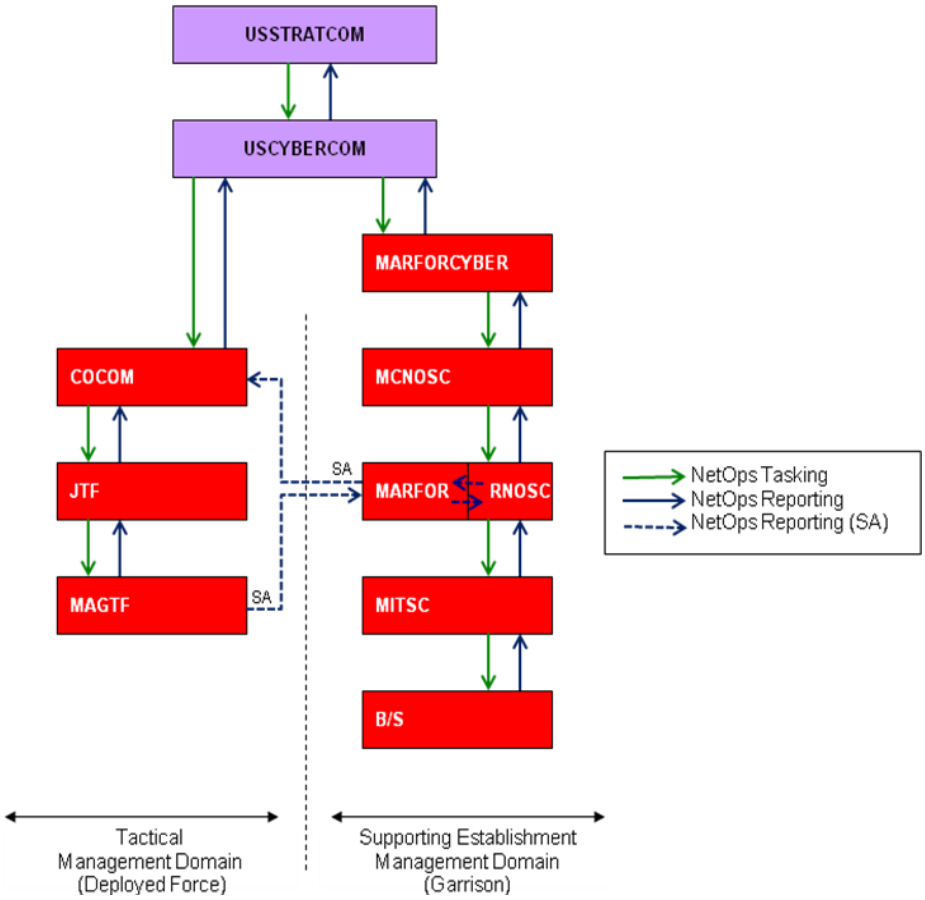

Figure 9: Global Tasking and Reporting

Though not shown in the figure, GCCs also issue directives to their Service Components to execute USSTRATCOM and USCYBERCOM direction. RNOSCs or MITSCs provide necessary reporting of regional compliance to their supported MARFORs and COCOM theater NetOps organizations (i.e. Theater Communications Control Center or TCCC) in accordance with supported COCOM Standard Operating Procedures (SOPs). Joint reporting systems are used where applicable or as they are developed.

RNOSCs and MITSCs must also report COCOM-directed changes up through the enterprise configuration management system or the USMC NetOps tasking and reporting framework to ensure accurate configurations are maintained. This allows the MCNOSC and subordinate commands to determine the impact of changes to the current network configuration.

Use Case #1 – Global USCYBERCOM Network Defense Direction

Scenario: A series of recent intrusions into DoD web portals that supports strategic force location and logistics planning has caused USCYBERCOM to issue a CTO directing that the specifically vulnerable portal software feature be immediately disabled since there is no software patch.

Action: The MCNOSC conducts an immediate operational impact assessment to determine whether or not terminating the particular portal capability will have an adverse impact to supported operations. The MCNOSC accomplishes this by accessing Configuration Management Data Bases to determine portal dependencies with associated applications, organizations, and missions and by querying the RNOSCs for an immediate operational impact assessment. RNOSC maintains situational awareness of current operations throughout the region and quickly assesses impact on operational forces. Feedback indicates that the particular feature of the software is not in widespread use and termination will only cause limited inconvenience. Through the tasking & reporting structure identified in Appendix G and using the Figure 10 flow of information, MCNOSC directs the Marine Corps to disable the portal capability. MCNOSC issues an Operational Directive to the RNOSCs and compliance reporting takes place through the RNOSC/MITSC reporting structure. This tasking and reporting includes deployed units. When the directed action is completed on all regionally managed systems, all RNOSCs report compliance to the MCNOSC who in turn reports global MCEN SIPRNet compliance to USCYBERCOM.

It should be noted that RNOSCs are also required to report globally directed actions to their regional chain of command. The RNOSC reports to the MARFOR and the TCCC supporting the COCOM that all Global SIPRNet assets (deployed and garrison) within their region are in compliance with the global directive from USCYBERCOM. For more on regional and deployed unit reporting see sections 2.6.3 and 2.6.7.

2.6.3. Regional Tasking and Reporting

Theater NetOps events are those activities occurring within a COCOM's AOR that have the potential to impact the operations in that theater. The affected GCC is the supported Command for theater NetOps events. USSTRATCOM, USCYBERCOM, MARFORCYBER and MCNOSC, as the Marine Corps Service NetOps component, provide support for theater NetOps events.

Regional tasking originates at the COCOM level and includes NetOps direction applicable to only the COCOM's AOR. Two clear tasking and reporting lines exist – one along the TMD and one along the SED. Additionally, situational awareness is provided from MAGTF to MARFOR for deployed Marine Corps assets/compliancy directly supporting the COCOM, RNOSC to MCNOSC for deployed and Garrison Marine Corps assets/ compliancy directly supporting COCOM, and MCNOSC to USCYBERCOM for situational and operational impact updates, as required. COCOMs do not own the SE infrastructure, but are authorized to task in certain permissible activities. This is discussed later in this section.

Regional tasking and reporting is executed by the MARFORs (directly supported by the SE) and their operating forces. Within the SED, the RNOSC is the primary NetOps organization supporting the MARFOR in the execution of regional NetOps; though in some cases, the MITSC fulfills this function. MARFORs issue regional OpDirs through the RNOSC/MITSC structure for execution by all operational forces (garrison) and all in-theater SE organizations. Network architectures and command relationships have been established to allow for the maximum regional support and compliance possible consistent with maintaining a globally integrated network. It is through a Direct Support command relationship between the MARFOR and Base Commanders that the MARFOR tasks the SE with executing regionally directed actions. Figure 10 illustrates this tasking and reporting.

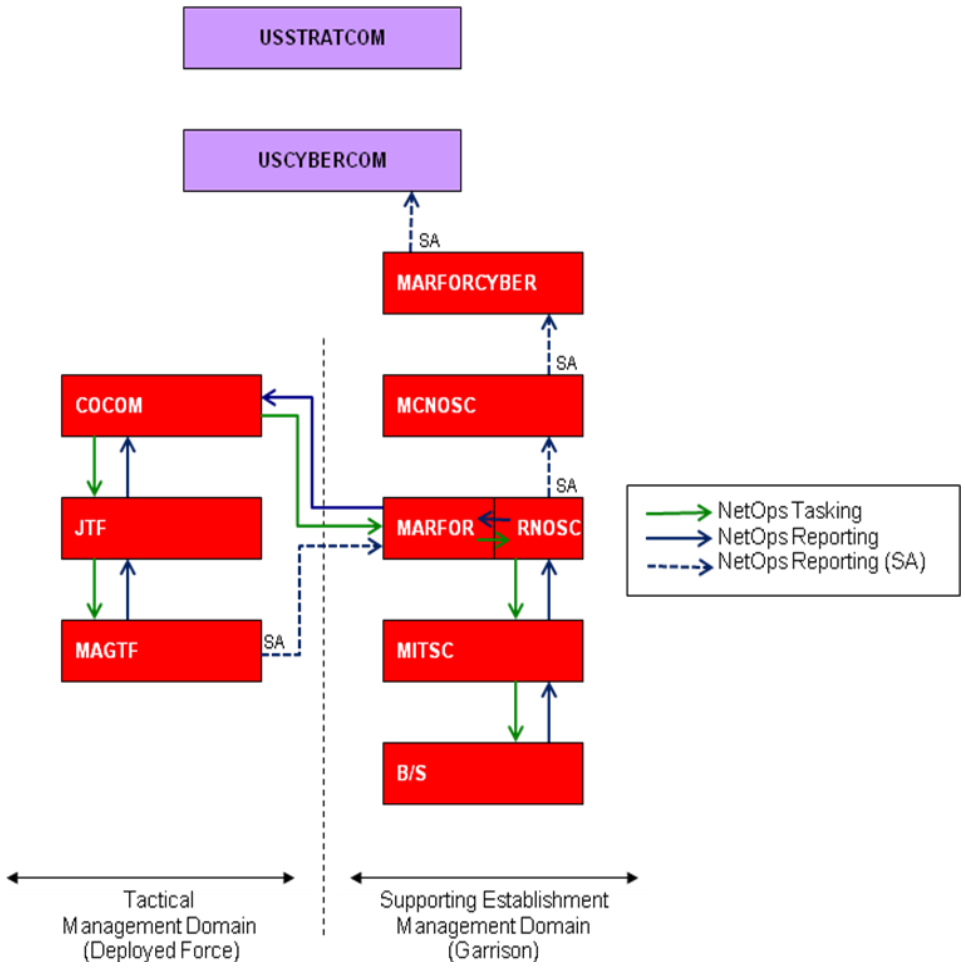

Figure 10: Regional Tasking and Reporting

Figure 11 provides a specific example of tasking and reporting for MARFORPAC. MARFORPAC receives PACOM direction[1] and issues direction through the RNOSC. Units in garrison receive tasking and report through the RNOSC/MITSC operations centers. Units in the field receive tasking and reporting through the RNOSC. More on C2 considerations for deploying units can be found in Section 2.7.3.

[1] Note: If a required action has effects outside of the region, it will not be performed unless directed by USSTRATCOM.

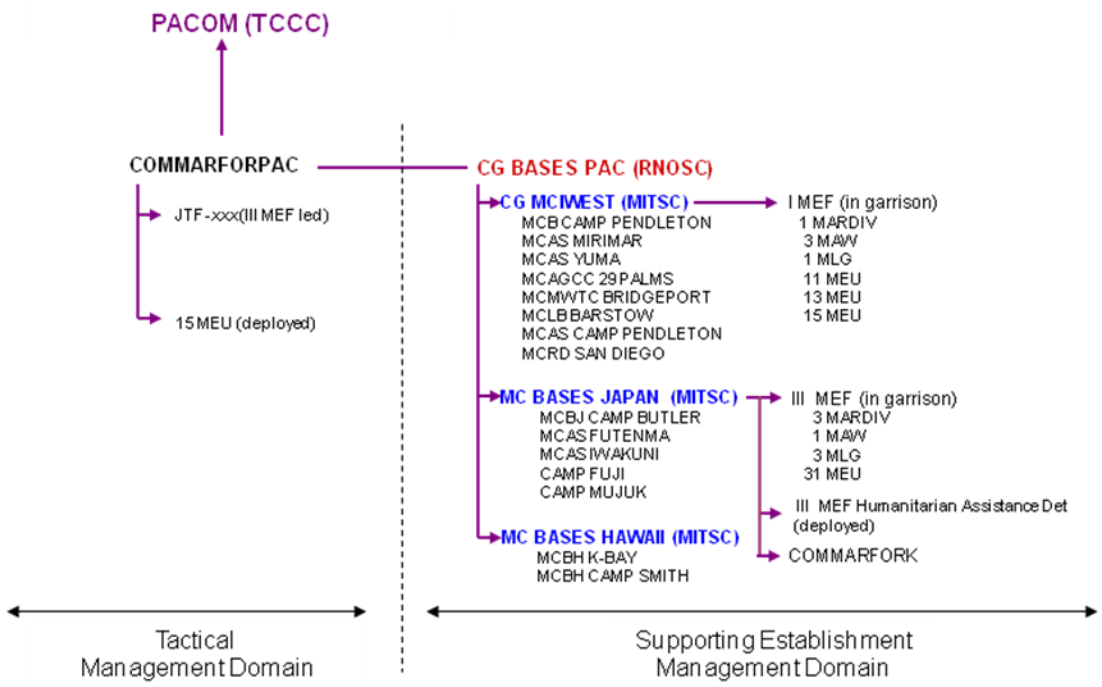

Figure 11: Example of MARFORPAC Tasking and Reporting

The MARFOR conducts a mission analysis and planning with major subordinate commands including those represented or directly supported by the MITSCs. The RNOSC (or supporting MITSC) directly supports the planning effort. Planning is coordinated with the MCNOSC as some directed actions directly involve or indirectly impact globally managed infrastructure in the theater. OpDirs are issued in accordance with the enterprise change management process, which determines if an action may have a unique impact to the MCEN Garrison SIPRNet operating environment and supported USMC organizations and missions. This includes regionally directed actions that may impact the global integration and effectiveness of the MCEN SIPRNet. Should a conflict arise between regional and global authorities, escalate the issue to the Service Headquarters and USCYBERCOM for resolution. The MARFOR, through the RNOSC, uses OPDRS to automate and standardize the reporting process as much as possible and to provide visibility of execution throughout the NetOps community.

As stated, regional events are events that by definition do not impact beyond the region. Similarly, regionally directed actions are actions that do not adversely impact the Global SIPRNet beyond the AOR. Should the COCOM direct an action that will have an adverse impact to the functioning of the Global SIPRNet by interfering with the operations of systems that operate across regional boundaries, then the directed action must be escalated to the MCNOSC for assessment, approval, and coordination. Further escalation to USCYBERCOM by the Marine Corps Service Headquarters will occur if the MCNOSC non-concurs with the action. However, the MCEN Garrison SIPRNet has been constructed with capabilities to allow for many types of operations executed regionally in response to the COCOM's direction. Examples of permissible activities:

- Validation and revocation of regional/local access controls
- Prioritization of the use of regionally allocated network resources (HW/SW, storage, bandwidth, etc.)
- Increases in regional INFOCON level
- CND Tailored Response Operations designed for local execution (log reviews, password changes, etc.)
- Certain CND Response Actions
- Support for deployed operations and exercises

Examples of activities that require approval and support from the MCNOSC, or that may be escalated to USCYBERCOM for resolution:

- COOP execution
- Directed modifications to B1/B2 configurations
- Establishing special trust relationships to external networks
- Directed changes to Marine Corps enterprise managed core services [Global Access List (GAL), Active Directory (AD) Global Policies, Public Key Infrastructure (PKI), etc.]
- Directed changes to enterprise managed user services
- Red Team operations
- Regionally managed application support

Use Case #2 – PACOM Directed INFOCON Change

Scenario: Given the current status of unrest in the Republic of North Korea and recent bellicose statements from unfriendly third world nations, PACOM has decided to raise the regional INFOCON level from 4 to 3. USSTRATCOM is considering raising DoD's INFOCON level, but has not done so yet.

Action: In advance of raising INFOCON levels, PACOM issues a warning order and solicits operational impact assessments. MARFORPAC, through its supporting USMC RNOSC (RNOSC Pacific) and supporting MITSCs conducts an ops impact assessment. The ops impact assessment also includes a separate assessment by MCNOSC concerning the ability to execute increased INFOCON on global systems managed in theater. The MCNOSC assessment confirms the ability to execute PACOM specified actions without adverse impact to MCEN managed systems and operations. As part of the increase in INFOCON levels, the pace at which systems in theater and those supporting theater operations receive refreshed baseline loads will increase, improving the readiness posture of the MCEN. This, however, generates the use of significant additional system and personnel resources. Fortunately, these added resource requirements are addressed in the MCEN Garrison SIPRNet systems architecture and organization and have been budgeted for in advance.

As a result of receiving feedback from Component Commands, PACOM issues direction to raise the INFOCON level from 4 to 3. MARFORPAC issues direction to USMC organizations throughout the AOR via tasking as shown in Figure 11. All organizations are directed to report reaching INFOCON 3 no later than a specified time. As indicated by Figure 11, garrisoned operating forces and SE organizations (B/S and tenant commands) report reaching INFOCON to the RNOSC via the MITSCs. Primary route for units managing deployed networks, such as JTF-501 and 15th MEU is to report to PACOM through their respective JTF or strike group and not the USMC RNOSC. However, tactical forces are still required to provide a courtesy report to the RNOSC for reporting to MARFORPAC. Additional description of deployed operations can be found in Section 2.7.3. The MCNOSC reports compliance of in-theater globally managed Marine Corps assets to the MITSCs. The RNOSC reports compliance to MARFORPAC and passes the report to PACOM TCCC for reporting to PACOM. Lastly, the RNOSC provides visibility of the status of theater wide INFOCON change to the MCNOSC.

2.6.4. Service Tasking and Reporting

Service tasking and reporting occur for events and actions directed by the Service Headquarters. These actions are generally aimed at fulfilling Service Title 10 responsibilities to install, maintain, and operate the SIPRNet, ensure the readiness of the Marine Corps to support future missions, and comply with DON and DoD direction.

Service tasking originates at the HQMC level and includes USMC NetOps direction applicable to USMC-only policy. One primary tasking and reporting line exists for USMC assets and compliancy. Additionally, situational awareness is provided from MARFOR to COCOM for situational and operational impact updates, as required, and from MCNOSC to USCYBERCOM for situational and operational impact updates, as required.

Figure 12 depicts the general tasking and reporting for Service directed NetOps. It is understood that Service directed actions may have the potential to affect on-going global and theater network operations and the missions they support. Therefore MCNOSC conducts mission analysis and planning with major subordinate NetOps commands including those represented or directly supported by the four RNOSCs. Service-wide operational directives are issued in accordance with the enterprise change management process, which determines if an action may have a unique impact to on-going operations of supported organizations. In accordance with the enterprise release and deployment management process, Service directed actions designed to maintain and upgrade the MCEN SIPRNet are targeted to specific infrastructure areas or phased into the environment to minimize overall impact to operations.

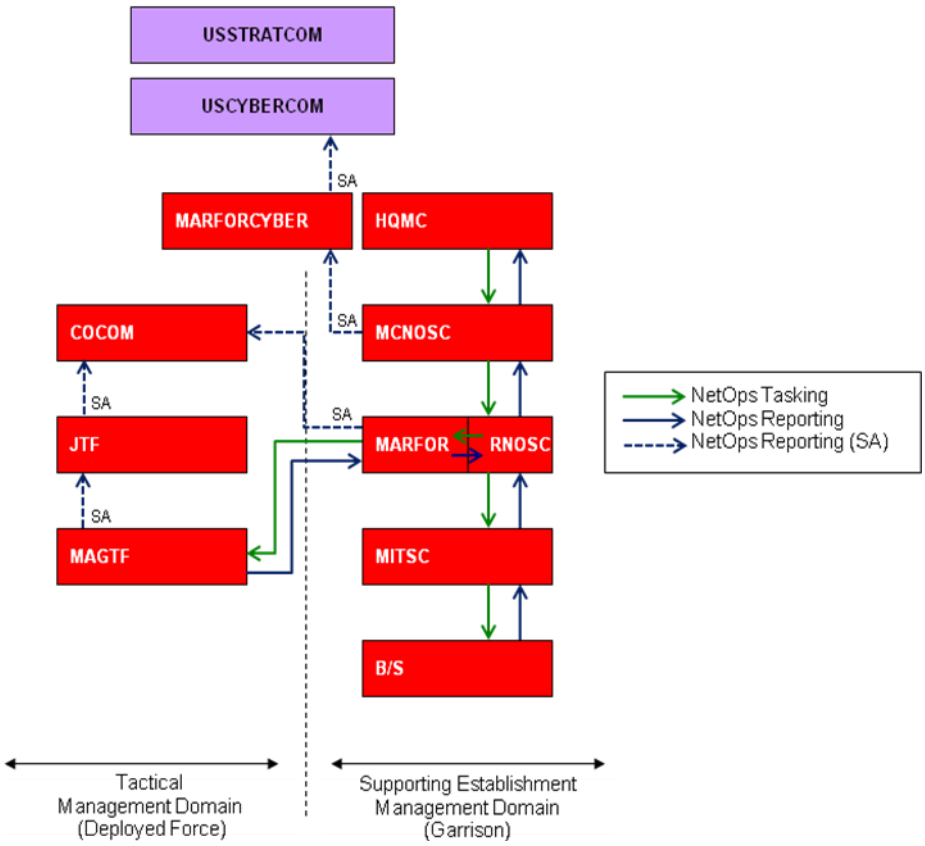

Figure 12: Service Tasking and Reporting

Use Case #3 – Marine Corps Directed Upgrade to Services

Scenario: DoD has directed that PKI be implemented within the GIG. As a result, the Marine Corps has established an acquisition PoR for PKI and planned a rollout of PKI across the MCEN SIPRNet to include the use of Common Access Cards (CAC) and tokens at the user level.

Action: To this point, governance and acquisition processes have addressed the need to define and prioritize the requirement for PKI, budget for the new capability, establish a PoR, design and test the architecture, and develop and implement policy, procedures and organizational changes necessary to field the new capability. Configuration Items (CIs) have been refined within the test environment and are ready for transition into the operational environment. In adherence to the RDM enterprise process, a deployment plan has been developed to field the capability in a phased approach, starting first with the deployment of infrastructure within the MCNOSC and MITSCs, and then a Service-wide program for mandatory training and issuance of CAC and tokens to users. The final step in the plan is a regionally phased CAC/token enforcement that precludes further access to the network via user name and password.

The plan includes deploying capabilities, training, and procedures to both the MCEN SIPRNet environment. Implementation/release plans have been carefully coordinated between Marine Corps Systems Command, the MCNOSC, and G6 community through the RNOSCs and MITSCs.

A formal Request for Change (RFC) has been submitted to Change Management, including a deployment package (containing the deployment plan) signed by stakeholders for this PKI deployment. After reviewing the package and ensuring that the deployment has been coordinated with other major changes in the Enterprise Change Schedule, the Change Advisory Board (CAB) approves the RFC, allowing the deployment to proceed as planned.

Over a series of months, and in accordance with the plan, the MCNOSC has issued direction via the RNOSCs for the Marine Corps to execute various actions required at the regional, sub-regional, and local level. The majority of these actions centered on support to end-users, including issuing CAC/tokens and validating the completion of training. Additionally, the MCNOSC ensured that new ESD capabilities were developed, tested, and trained. The direction included support for upgrading tactical unit equipment and procedures as these units return from the field. Each directed set of actions/milestones is tasked and reported through Figure 6 chain of command via Figure 12 flow of information.

Because much of the Marine Corps core infrastructure is managed by the MCNOSC, implementation of core PKI and enforcement of users has not been directed to the RNOSC/MITSCs. Instead, MCSC has worked with the MCNOSC for implementation of this infrastructure. As approved changes are carried out, CIs are updated in the CMS. Even though the deployment package has been approved by Change Management, the MCNOSC has continued to coordinate with the RNOSCs to ensure there is no operational impact before issuing Operational Advisories concerning specific implementation dates and maintenance outage periods for the planned release of capabilities. The last step in implementation includes MCNOSC executed phased enforcement of users. This step is very closely coordinated with the RNOSCs to ensure no adverse operational impact. If RNOSCs or Incident Management indicate unforeseen errors in the deployment, the back-out plan is executed.

2.7. COMMAND AND CONTROL – MORE ON SUPPORT RELATIONSHIPS

The RNOSC/MITSC structure is designed to execute the NetOps mission and in doing so provide effective support to Marine Corps organizations and missions. However, supported commands share in the responsibility with NetOps organizations to make the mission a success. The following sections describe additional considerations and the roles and responsibilities for supported tenant commands, application managers and deploying units.

2.7.1. Tenant Command Support and Responsibilities

Tenant commands aboard B/S are provided IT services by their supporting MITSC and Base G6s. Appendix G lists the tenant organizations, their C2 structure, and the SE commands providing support. Although in many cases, NetOps tasks are directed to commands that operate NetOps support centers or local B/S G6's, there are cases where supported tenant commands have responsibility for supporting NetOps missions and mission tasks. In such cases, the supported command becomes a supporting command. Appendix G provides a detailed list of commands and the MITSC/RNOSCs they report through. The following cases illustrate how and when tenant commands are tasked with supporting NetOps execution.

- Supported commands are responsible to identify unique mission support requirements, and request those required supporting services through the Appendix G chain of command. While the MITSC and supporting B/S establish and manage SLAs for support, it is incumbent upon supported commands to identify when SLAs are inadequate or when additional services are needed. Specific methods tenant commands will use to report many of these requirements will be identified and tied together through the Enterprise Information Technology Service Management (E-ITSM) effort.

- Supported commands are responsible for participating in and providing input to NetOps mission planning conducted by RNOSC and MITSC commands. Input on mission impact of proposed actions, including routine maintenance outages, mandated security response actions, INFOCON changes, changes in priorities for planned service upgrades, and other operations is essential for effective NetOps execution.

- Supported commands that retain TechCon of local applications or devices on the network must operate them in accordance with all NetOps taskings. In such cases, supported local commands must register all devices and applications, ensure approval to operate on the network (i.e., Certification & Accreditation), ensure visibility of all locally managed systems within the MITSC, and comply with all NetOps direction issued through the RNOSC/MITSC structure.

- Effective NetOps relies upon trained and knowledgeable end-users and service providers. Supported commands must comply with mandatory NetOps training requirements and security stand-downs. Locally supported systems must be maintained by qualified service providers. Special training requirements may be issued by the NetOps chain of command. Compliance is tracked and reported through the G/S6 structure.

Supported commands will ensure all command and end-user actions necessary to execute a NetOps mission or mission task are completed. Many NetOps security tasks involve ensuring appropriate access controls be maintained or increased at the local command level. Control of access to local systems and command data are a supported command responsibility and identification of suspicious activity on the network is an end-user responsibility. Additionally, many INFOCON tasks and Tailored Response Options (TRO) can only be executed with support from local commands and users.

RNOSC/MITSC commands will ensure the integration of locally supported commands into effective NetOps C2 and mission execution. In order to do so, RNOSCs and MITSCs must track all supported commands, associated missions and specific IT systems supporting those missions, and the number and locations of command users. The Marine Corps operational environment is highly mobile and constantly changing making this a challenge; however, effective NetOps demands adequate situational awareness and focus on supported mission. The MITSC will report end-user devices and IT systems it directly manages in support of these commands. At the same time, the MITSC will require disciplined management and reporting for locally managed IT systems connected to the garrison network.

2.7.2. Applications Support

Applications are supported in a variety of enterprise, regional, and local environments that include services and systems that connect to and operate on the network. Many applications and associated data stores remain operationally stove piped. Some are supervised at the enterprise level by various Marine Corps FAMs. Other applications and associated data are managed regionally in support of regional SE command and operating force missions. These applications may be unique to requirements of regional command authorities such as a supported COCOM or unique Joint or coalition environment. Still other applications are locally managed, created to support emergent mission needs of the organizations they support.

The Marine Corps has established a goal of creating an effective and integrated applications support and shared data environment. Such an environment will ensure more effective and secure sharing of data and information across the network. In order to achieve this goal, the Marine Corps Enterprise Information Technology System, Program of Record has been created. MCEITS will accomplish this goal by implementing an IT infrastructure with an Enterprise Application Environment (EAE), and an Enterprise Service and Data Environments (ESDE) within the EITCs, but extended to the regions and TMDs (deployed forces).

This application and data infrastructure will quickly and easily adapt to the evolving software, hardware, data, services, and management requirements while providing an enhanced enterprise visibility, security, and management discipline that facilitates greater reuse of IT assets. The intent is to provide responsive support for a secure, collaborative, interoperable data sharing environment while enabling the integration of products, services and users. These capabilities support and contribute to the DOD's overall GIG Enterprise Services (GES) and Net-Centric Enterprise Services (NCES).

The Marine Corps vision is to create an environment where all enterprise applications are supported within the EITCs with appropriate connectivity and access to federated DoD systems and data. At the same time, regional and local applications can be supported within the MITSCs with appropriate access and connectivity to common data at the enterprise level. Tactical applications can also be supported by the EITC/MITSC data center structure, as well as in the field. Over time, most Marine Corps applications and data are to migrate to this common operational environment. Support will be provided under SLAs between USMC NetOps organizations and application service support centers and the organizations they support.

Specifically, application support is provided through the Enterprise Service Desk using the Incident Management process. Application users requiring support call the ESD to initiate the trouble ticket. The ESD will resolve the issue if they are able to do so given their existing knowledge system or, transparently to the user, assign the ticket to the respective application service support center (i.e., MCEITS or one of the other MCSC PoRs.) Provision of this support through the ESD supports enterprise-wide incident reporting and trending. Additionally, the ESD is in the best position to identify if the incident is in fact an application-related or associated with a network, hardware, or other connectivity issue, in which case the trouble ticket can be subsequently passed to the appropriate MITSC for resolution. For more information on the Incident Management process, refer to section 4.5.3. and the E-ITSM Incident Management Process Guide.

Until the Marine Corps transitions to the MCEITS operational environment, enterprise, regional, and local applications and associated data stores will remain supported by their current organizational sponsors until respective planned migration is complete. In order to support effective NetOps C2 of these mission essential capabilities, the following requirements apply to applications owners. These requirements are similar to those for supported tenant commands.

- Supported application owners are required to identify unique mission support requirements. MITSC and supported B/S establish and manage SLAs for support in accordance with established service level management processes and enterprise wide standards. It is incumbent upon supported commands to identify when SLAs are inadequate or when additional services are needed. Application owners are responsible for requesting supporting services to meet mission requirements.

- Application owners are responsible for participating in and providing input to NetOps mission planning conducted by RNOSC and MITSC commands. Input on mission impact of proposed actions, including routine maintenance outages, mandated security response actions, INFOCON changes, changes in priorities for planned service upgrades, and other operations is essential for effective NetOps execution.

- Application owners operating devices on the network must do so in accordance with all NetOps tasking. FAMs, PMs, functional, and operational commands must register all devices and applications, ensure approval to operate on the network (i.e., Certification & Accreditation), ensure visibility of all managed systems within the MITSC, and comply with all NetOps direction issued through the RNOSC/MITSC structure. Additionally, these commands must ensure timely approval and support for patching all applications to comply with directed IAVA patching.

- Application owners must allow routine scanning of devices operated on the network to ensure compliance with NetOps direction and to identify vulnerabilities and threats to the network. Scanning may be conducted by the MCNOSC or RNOSC/MITSC NetOps organizations. Appropriate coordination and planning for announced and unannounced scans will be conducted between scanning organizations and application owning organizations to ensure there is no disruption of applications services essential to on-going missions.

The status of enterprise applications will be made available to all RNOSCs/MITSCs via NetCOP and other common management tools. All MITSCs will operate under standard Marine Corps-wide SLA for support to regional application owners and will coordinate planning and execution of NetOps to ensure actions do not disrupt application services during times of critical mission support.

2.7.3. Support for the Operational Forces in the Tactical Environment

The regionalization concept and C2 reporting structure outlined within this document are designed to provide support to Marine Corps OPFORs, both in garrison and deployed. This includes the seamless transition from a non-deployed status to deployed status and back again. Users should retain the use of same username, password, and e-mail address, as well as access to individual storage space (home drive), organizational shared file systems, and portals. OPFOR requirements, regardless of the operating environment, remain the same. An operational unit is considered in a deployed state under either of the first two conditions identified in Table 1. An operational unit is considered in a non-deployed state under any other circumstance. Non-operational and SE units are all considered non-deployed.

Table 1: Deployed Status Conditions

Status	Condition	Service Provider
Deployed	Physically located off a garrison Marine Corps installation for the purpose of executing an operating force mission. The transition begins 60 days before users leave the non-deployed environment. Transition back to a non-deployed state completes 30 days after returning to the installation.	MEF G6
Deployed	Tactically located on a Marine Corps installation for the purposes of conducting exercises or training. The transition begins 30 days before the start of exercise (STARTEX), and transition back to a non-deployed state completes 30 days after the end of the exercise (ENDEX).	MEF G6
Non-Deployed	All other conditions	Regional MITSC

2.7.3.1. MCEN Active Directory (AD) Services

The SIPRNet has been designed to support a single AD forest containing multiple domains[1]. The Marine Corps World-Wide (MCW) domain was established to support garrison users. The operational force and child domains were created to support the major subordinate commands. This AD structure provides the ability to meet the requirements mentioned above for seamless end-users services in both deployed and non-deployed states.

[1] The use of the term domain here should not be confused. A "Management Domain" (MD) is a NetOps reporting structure and a "domain" within active directory is part of a logical framework.

Figure 13 below is a high level view of this AD structure.

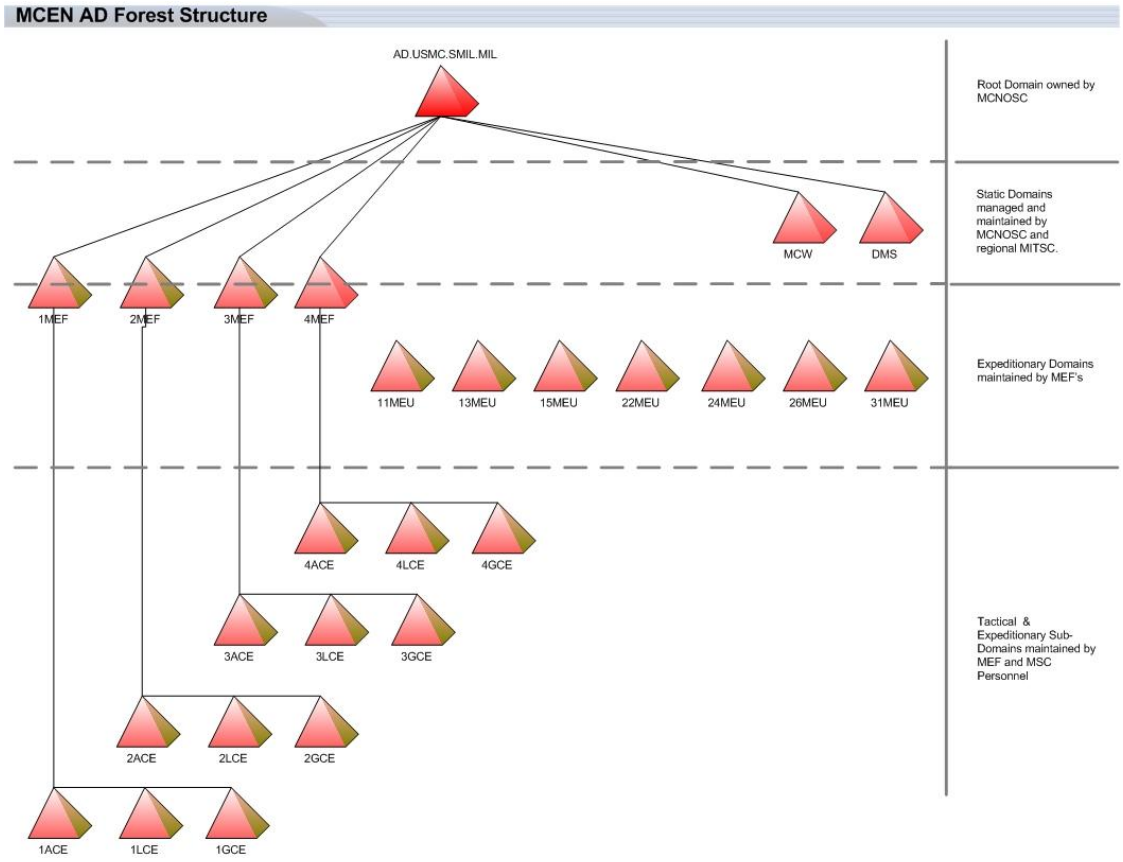

Figure 13: Marine Corps Worldwide Active Directory

SE users will always reside in the MCW AD domain. OPFOR users will always reside in their expeditionary domains. Economy of effort being the goal to maintaining a stable and consistent presence across the MCEN, network design will facilitate the same look and feel in respect to network applications and user viewable information.

Given the distributed operational capabilities inherent within AD, domains no longer need to be restricted to a single physical site. They can be managed, with the use of permissions, by two or more management organizations for the purpose of providing the OPFOR user with a familiar network experience in the field or while operating in garrison. OPFOR users working in a non-deployed status will reside in the expeditionary domain, but will be placed in an OU hierarchy managed by a regional MITSC where the supporting establishment domain maintains administrative control, technical control, and NetOps reporting responsibilities. While MEF G6 personnel manage the domain itself for reporting and administrative responsibilities during both deployed and non-deployed periods, the OU structure is reportable in accordance with the regional NetOps chain, and administratively functional for the regional MITSC support staff to effectively manage all users that fall in a non-deployed status within its region.

Expeditionary domain OU structures will mirror the structure (not actual names due to unit and MSC naming differences) of the MCW OU hierarchy to facilitate the permissions required to allow the MITSC support staff from the MCW domain to administrate OPFOR users in the expeditionary domains. All permissions outlined in the MCNOSC Delegated Permissions and Security Guide will be applied to the OPFOR domain SE OU hierarchy to provide a known framework of permissions and adhere to the economy of effort methodology.

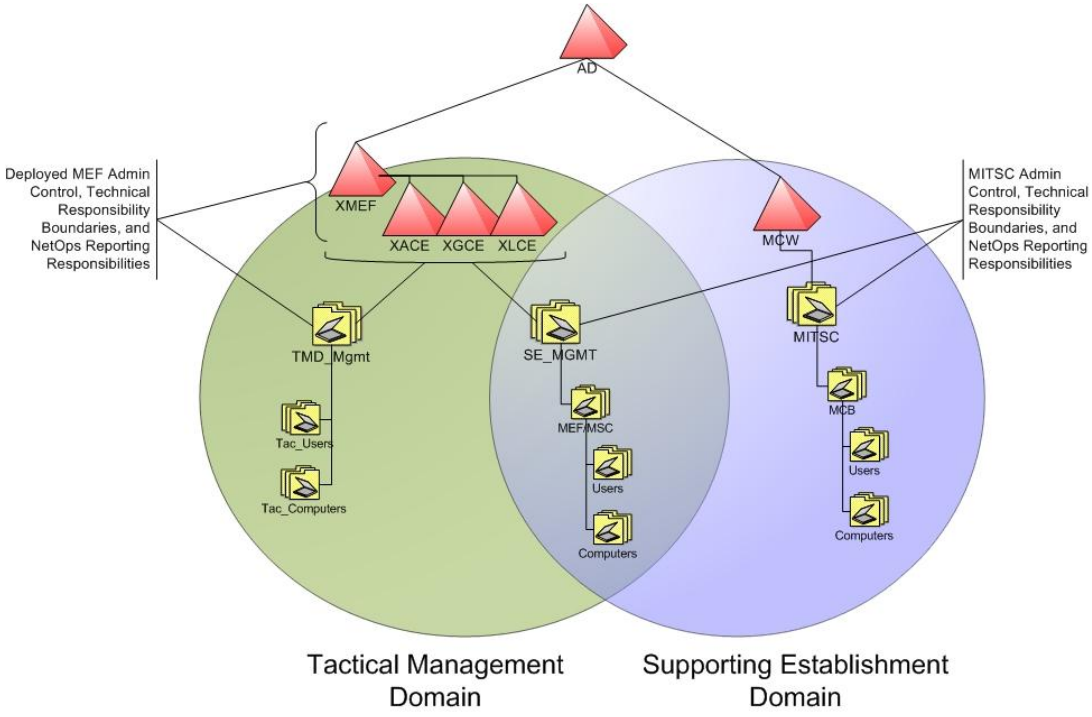

Figure 14: AD Responsibility Boundaries

The process of moving personnel to/from the expeditionary domain has two different scenarios:

- Migration between the expeditionary domains due to deployment requirements
- Migration to/from MCW domain due to Permanent Change of Station (PCS) or Permanent Change of Assignment (PCA).

Both scenarios require a carefully planned and managed transition process in order to conduct a smooth transition of user accounts and data (including mailboxes). Additionally, both necessitate contact with the regional MITSC to first establish a RFC to ensure proper Configuration Management records are kept and to ensure auditing is being conducted. The required permissions and procedures will be specified in the MCEN Intra-forest User Migration Procedures ITI to be published separately. While no static document can encompass all possible future migration scenarios, this ITI will outline the most anticipated scenarios based on unit size, time requirements, and transport bandwidth/delay issues.

2.7.3.2. Expeditionary Domain NetOps Reporting[1]

NetOps reporting is delineated in the OU structure that computer objects requiring compliancy are located. All deployed computers and servers will reside in a tactical management OU hierarchy managed by either deployed network defense suites or the network defense services offered by the regional tactical NOC and reported on by the MEF NetOps reporting chain. The actual date upon which responsibility for reporting transitions from the USMC (MITSC NetOps reporting chain) to the COCOM (Deployed MEF) is defined by the realignment of forces as specified in the COCOM Operations Order (OPORD.) Reporting reverts back to the MITSC NetOps reporting chain when the Deployed MEF is officially transitioned back to the USMC. In the absence of an OPORD, responsibility for NetOps reporting remains with the Supporting Establishment. The domain itself, for the purposes of NetOps reporting will be the responsibility of the MEF G6 as the AD domains themselves potentially span more than one NetOps reporting chain. All non-deployed application servers and client computers requiring compliancy reporting will be located in the supporting establishment OU hierarchy where the regional MITSC has the ability to effect group policy changes and software updates. The MITSC NetOps reporting chain will be responsible for reporting all servers and clients within their supporting establishment OU hierarchy. PoR systems, applications, or data stores are an exception to this rule. Refer to section 2.6.1 for additional information on tasking and reporting.

[1] The use of the term domain here should not be confused. A "Management Domain" (MD) is a NetOps reporting structure and a "domain" within active directory is part of a logical framework.

3. NETWORK COMMON OPERATIONAL PICTURE (NETCOP)

NetCOP is a subset of the enterprise ITSM toolset, and is used to display integrated and customized views of the status, performance, events, threats and vulnerabilities for certain aspects of the Global SIPRNet and all of the MCEN SIPRNet. The views range from high-level global views down to more granular views of each region, base, LAN, command, and end device. The primary purpose of NetCOP is to present NetOps personnel with SA of MCEN SIPRNet services in near real-time in order to interpret events, incidents, and problems; understand their operational impact; and decisively and rapidly take action to restore services and protect information on the MCEN SIPRNet. NetOps SA for the MCEN SIPRNet is derived from common reporting requirements using functionally standardized enterprise-wide management tools and common data information exchange formats. These tools collect, and correlate information in real time or near-real time to produce defined views or initiate automated processes.

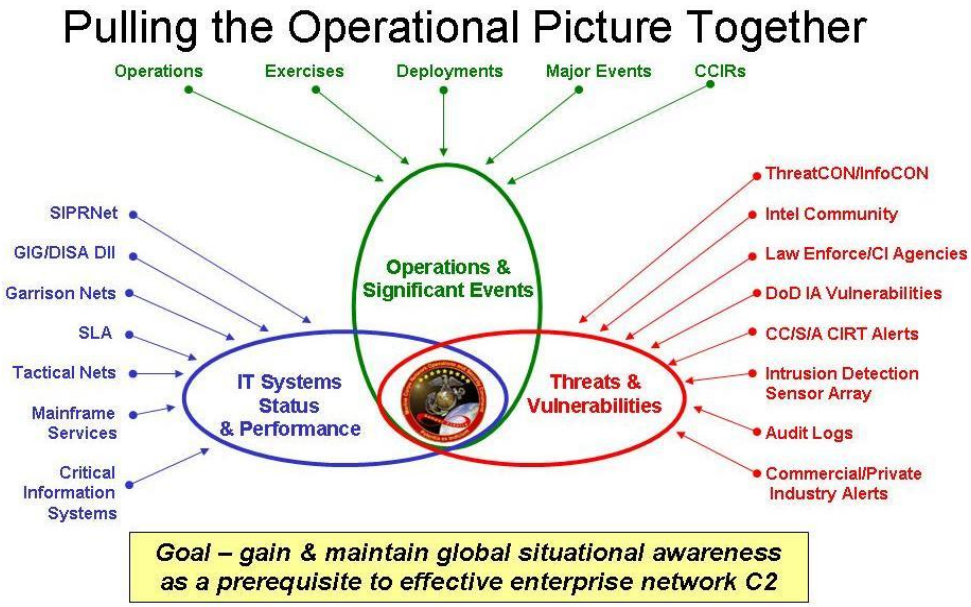

Figure 15: NetOps Situational Awareness

As depicted in Figure 15, USMC NetOps SA covers three areas: IT Systems Status and Performance, Threats and Vulnerabilities, and Operations and Significant Events.

IT Systems Status and Performance provides an understanding of how the Global and the MCEN SIPRNet infrastructure and systems that depend upon it are performing (bandwidth, CPU, storage, and other resource utilization) in relationship to established SLAs. SA in this area is fed by Event, Incident, Availability, Capacity, IT Service Continuity, Information Security, Service Level, and Configuration Management processes and systems.

Threats and vulnerabilities come from many sources. Against the back drop of systems performance, network defenders must be vigilant to existing vulnerabilities within the systems and the status of patching these vulnerabilities. Vulnerabilities take on new meaning when there is an observed threat or exploit available and in use on the Internet. In such cases additional actions beyond patching may be necessary to mitigate the threat. SA in this area is fed by Event, Incident, Availability, Capacity, IT Service Continuity, Access, Information Security, Release and Deployment, and Configuration Management processes and systems.

Operations and significant events must be correlated across the enterprise. Perhaps most importantly, they provide awareness of who is using networked systems and for what purpose. Marine Corps operational organizations must know the applications and data, types of network communications used, locations and units affected, and associated military operations they are undertaking to complete the picture. Operations and significant events are inputs to Event, Incident, Availability, Capacity, IT Service Continuity, Access, Information Security, Release and Deployment, Service Level, and Service Asset and Configuration Management processes and systems.

When this information is properly captured, processed, integrated, and analyzed, IT operations can appropriately interpret network activity and prioritize network operations support to ensure the warfighter remains effective. This type of SA is invaluable, and can be used to support other types of military operations. Indications from the network sometimes precede other Indications and Warnings (I&W) of unfolding operational events.

3.1. NETCOP CONCEPT

To assemble NetOps SA information, NetCOP correlates data from multiple sources as part of the overall ITSM toolset. Event Management tools monitor and poll service components and configuration items such as network elements, storage devices, applications, and critical network services. NetCOP correlation engines also map multiple event notifications into smaller, collective events to aid human comprehension. Visualization tools provide different types of views (overlays) of services, devices, and software at varying levels of granularity.

Events and incidents also feed the Availability and IT Service Continuity Management engines, which support trending analysis for predictive assessment and actions. Situational awareness includes not only immediate actions, but also the ability to understand long-term performance trends and determine the future state of the network and its services.

These elements of situational awareness allow NetOps organizations to measure how well their networks and systems are performing and to measure this performance against one or more service level targets, which are defined in established SLAs. Using NetCOP to measure the operating environment in relationship to SLAs provides the necessary awareness for maintaining service for supported users. NetOps SA includes reports, and displays the service provider's ability to meet established service levels and provides incentive to continually improve service.

The overall concept for NetCOP is depicted in Figure 16 below. The bottom of the figure depicts elemental data. It is monitored and managed by several systems, tools, and processes. Once collected and assembled, that information is fed up to systems that aggregate and correlate the various feeds to parse relevant details. The information is then presented in customizable formats for various users and operators.

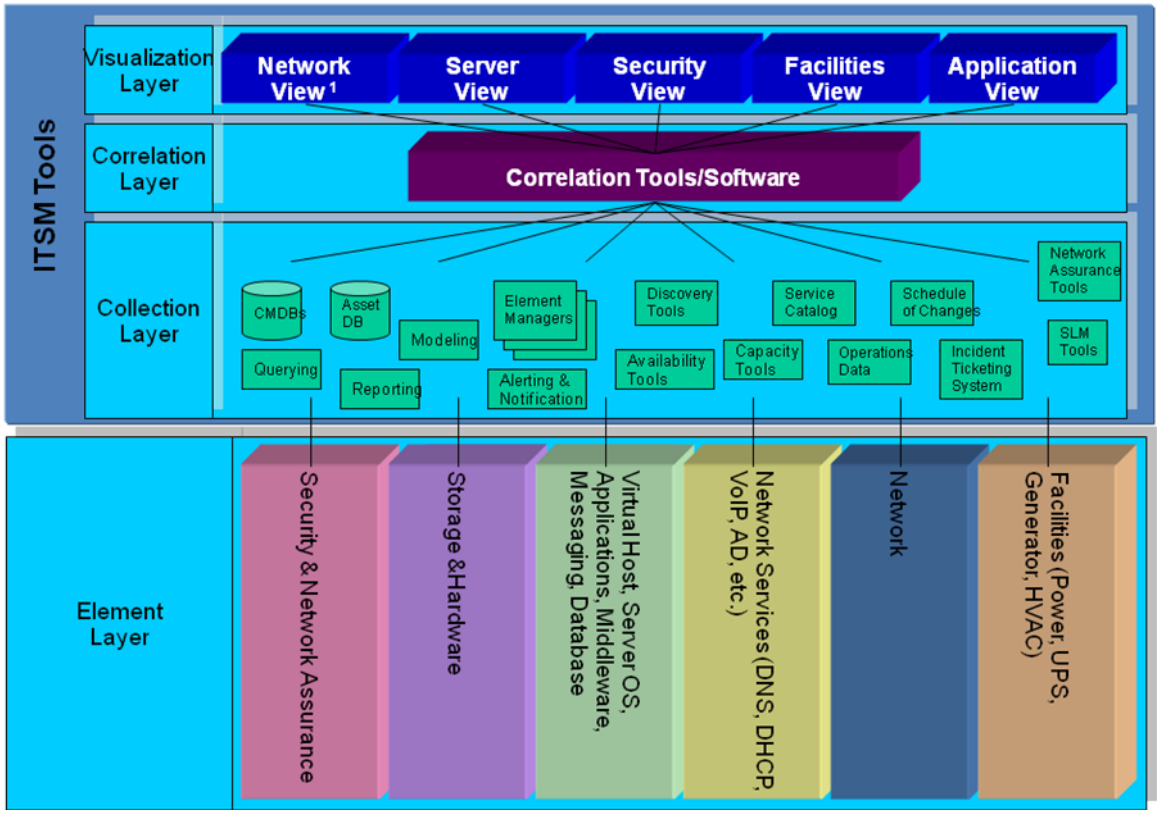

Figure 16: NetCOP Concept

NetCOP data is pulled from collection layer tools that manage specific elements or groups of elements. Each element management tool provides a varying degree of capability including: Event, Availability and Capacity Management, Discovery, and Network Assurance. Availability and Capacity Management tools evaluate and report on the behavior and effectiveness of elements.

[1] 'Network View' goes down to and includes user workstations.

Event and Incident Management tools enable corrective action for an error or anomaly on a particular device. Configuration Management tools document information about a device and its settings. Network Assurance tools provide information on the security posture of a device. When information from these tools is assembled, it provides a complete picture.

Correlation tools are employed to bring together all the various feeds and to logically link incidents and events. Overall, ITSM is enabled by combining all devices and their dependencies, thus completing the network operational picture. It is crucial to ensure information from all sources is correlated in order for ITSM personnel to anticipate issues (e.g., capacity and availability), to quickly identify the source of a problem, and to restore service.

Finally, the information is presented in customizable formats for various users and operators. NetCOP provides views, such as network, server, security, facility, and applications. Local and Global administrators have tailored access to view and run reports from the central collection points. For example, a MCNOSC network analyst can review network devices and connections globally across the Garrison SIPRNet to help understand the current state, troubleshoot perceived problems, and remain proactive. NetCOP provides varying levels of service management perspective, situational awareness.

Network views are the most common and most familiar to network administrators today. They generally display routers and switches and their connections via a Simple Network Management (SNMP) or PING tool, such as Spectrum, Solar Winds, What' Up Gold, etc.

Server views show the status and connectivity of the servers and the services that reside on them. For example, one of these global views may show the grid of mail servers connected via their Lightweight Directory Access Protocol (LDAP) links, which show Active Directory (AD) flow.

Closely related server views are applications views which show the status and availability of network applications. Since applications are the real drivers for the networks, it is important to know how well the network supports or provides access to the applications. When an incident affects the network, it is important to also see what applications and services are being affected by the incident.

Security views will show active or suspected security related incidents, such as Denial of Service attacks. This information is not only important to network assurance personnel, but also to NetOps personnel, because in many instances network or service outages may result from security incidents and its important for NetOps personnel to quickly determine the source of a problem affecting the network and services.

The facility views are crucial to NetOps in terms of monitoring their status. It is important to know if power and climate control are functioning optimally and providing a healthy environment for our network and services. Knowledge of power or HVAC failures is crucial when trying to determine the cause of systems performance issues or outages.

A map that shows everything can get very busy and will provide no information to NetOps personnel. By creating various views or overlays, NetOps personnel can easily parse through the abundant visual information to focus efforts in troubleshooting or verifying overall systems performance. And because application availability relies upon the service, server, network, and ultimately facilities, it is particularly important that the

3.2. AVAILABILITY OF NETCOP

NetOps forces throughout the MCEN Garrison SIPRNet will have access to NetCOP capabilities, including aggregation, correlation, and visualization. MCNOSC (including the ESD and MCNOSC Detachments), RNOSCs, MITSCs, B/S G6, and Tenant G/S6 will have access to views of the SIPRNet at their corresponding organizational level and below, as well as one level above. Certain organizations will also have access to adjacent organizational views, at the discretion of the senior NetOps organization.

These tools will also allow administrators to remotely manage and configure designated devices within their respective areas of control. This will allow IT operations to leverage NetCOP views for event responses and resolution of incidents and problems. However, this type of control is not outside Change Management (although it may involve standard or emergency changes.)

3.3. **NETCOP ROLES AND RESPONSIBILITIES**

Table 2: Roles and Responsibilities[1] Table for NetCOP

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for NetCOP	CP	RA	C	C	C	C	C	C
Identify NetCOP requirements	RA			P	CP	CP	C	C
Validate NetCOP requirements	P	RA		P				
Develop NetCOP architecture	CP		RA					
Resource		RA	C					
Procure NetCOP tools	CP		RA					
Deploy NetCOP tools	CP		RA					
Manage and configure NetCOP tools	RA		I					
Configure devices/services to be monitored and managed by NetCOP tools	RA		P		CP	CP	C	
Manage devices/services with NetCOP tools	RA				CP	CP	C	
Develop customized views of SIPRNet using NetCOP tools	RA	I	I	R	CP	CP	C	C
Provide lifecycle management for the NetCOP tools	CP		RA					

[1] Note: At the time of this COE writing, the USMC E-ITSM process development effort is still in progress. The services and processes described in this document will be incorporated as the concept for ITSM is refined. In the interim, process flow diagrams for many processes are available in the SIPRNet Transition Plan published 23 December 2008 by HQMC. .

4. SERVICE MANAGEMENT CONCEPTS, ROLES, AND RESPONSIBILITIES[1]

4.1. FRAMEWORK

ITSM, as initially described in Section 1, is a discipline for managing IT systems that is philosophically centered on the user's perspective of IT's contribution to operations. ITSM focuses on providing a framework to structure IT-related activities and the interactions of IT technical personnel with users. The greatest benefit of ITSM/ITIL is an effective IT alignment with 'business' requirements and the customer focus which that demands. It also goes a long way to mitigate stove-piped Service solutions and operations, defining a common terminology, and clearly defining roles and responsibilities. Given the cross-organizational aspect of the USMC IT Service lifecycle, this last benefit may be particularly important. ITSM is the framework through which NetOps (IT Operations) is achieved and IT services will be delivered.

Due to current alignment of authorities (acquisition, policy, sponsorship, etc.) in the USMC, our ITSM framework must leverage a cross-organizational approach requiring a common understanding of roles and responsibilities, active process ownership, utmost cross-organization cooperation and participation, and leadership from the Service Strategy community.

This section focuses on describing in more detail the concepts and organizational roles and responsibilities for Marine Corps ITSM capabilities. These capabilities take the form of tailored ITIL functions and processes for managing IT services across the ITILv3 Service Lifecycle and over the lifespan of the respective IT Service. The following section identifies the lead and support roles within the Marine Corps by ITILv3 lifecycle stage. It will first address those functions and processes supporting Service Strategy where IT governance organizations typically take lead. It will then address the functions and processes supporting Service Design and Service Transition, where the IT Acquisition community typically has lead. Next, it will address the functions, processes, and major categories of USMC SIPRNet services currently in Service Operations. This section will conclude by addressing the continual need to evaluate and improve all functions and processes from all lifecycle stages.

[1] Note: all sections pending updates from E-ITSM effort (to include Roles and Responsibilities tables) are not actionable until post E-ITSM modifications are complete. As the process guide is completed for each process, Section 4 details will be removed from the COE and a reference to that guide will be inserted in its place. At that point, those roles and responsibilities will become actionable.

Another consideration is that ITSM in the Marine Corps is executed from an enterprise perspective. Figure 17 below notionally shows how all ITSM processes will support all IT Services used on the SIPRNet.

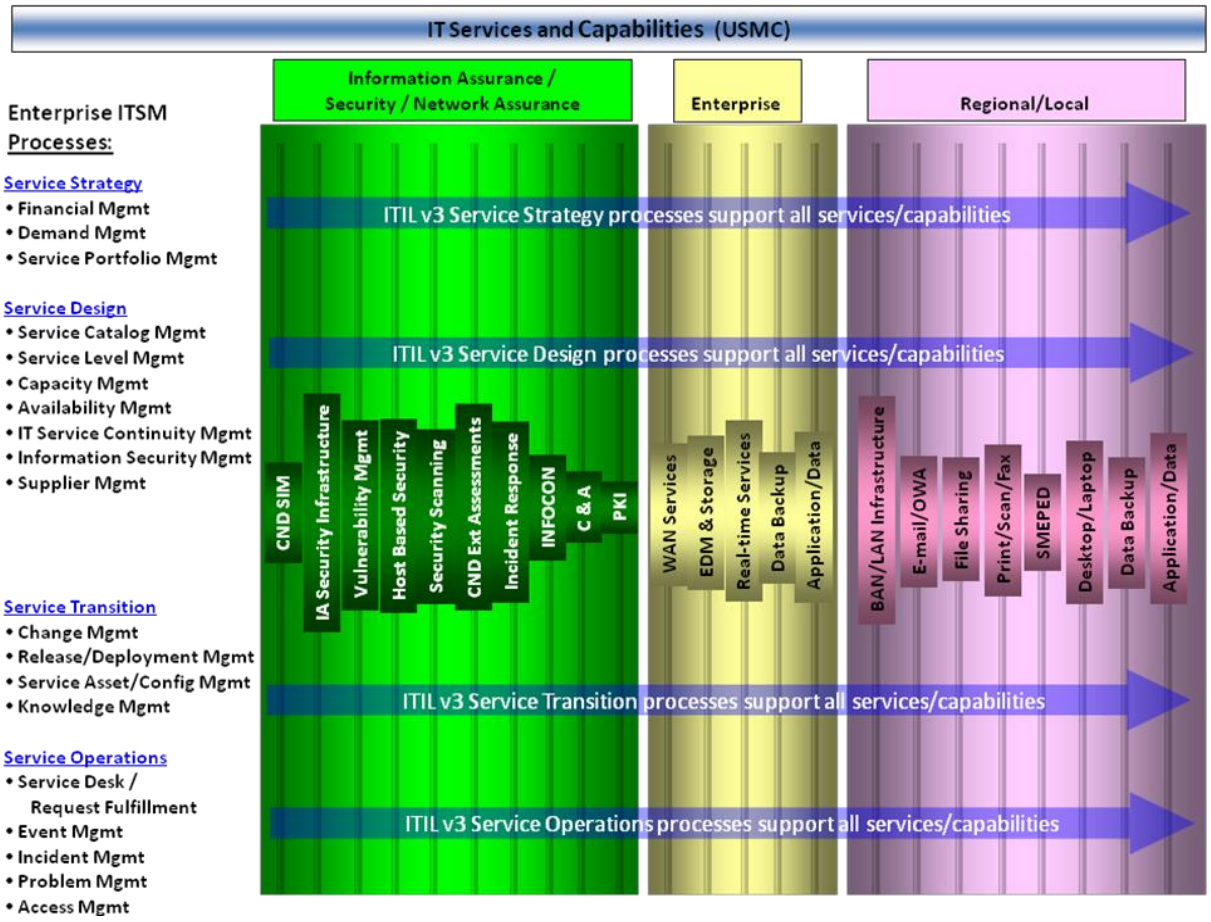

Figure 17: IT Services and Capabilities

4.2. SERVICE STRATEGY (IT GOVERNANCE)

The purpose of Service Strategy is to conduct the financial, business process, and current IT environment reviews and assessments in conjunction with current and future business requirements to provide strategic direction, financial support, and ensure IT integration with the needs of the business owners. Marine Corps business ownership (customer) consists of FAMs and the warfighter community. Marine Corps' Service Strategy roles and functions align with HQMC C4 who collectively executes these functions on behalf of CMC.

4.2.1. Financial Management

Financial Management tasks include assessing the overall value of an IT service, the costs of underlying assets associated with its provisioning, and its impact on Marine Corps-wide operations.

4.2.1.1. Objectives

Financial Management supports financial visibility and accountability, financial compliance and control, enhanced decision making throughout an IT services complete lifecycle, and a far greater understanding of the costs of providing a service and the value to the Marine Corps. In other words, assessing cost-benefit value and projected Returns on Investment (ROIs) before making a decision to move forward with establishing a new IT service capability to ensure that limited USMC IT resources are most effectively used.

4.2.1.2. Roles and Responsibilities

Table 3: Roles and Responsibilities Table for Financial Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for financial management	C	RA	C	C	C	C	C	C
Manage SIPRNet service portfolio		RA						
Ensure compliance with agreed upon accounting methods and practices		RA						
Provide acquisition and technical inputs	CP		RA	C				
Provide service valuation, accounting, and tracking of service expenses	CP		RA	P	P	P	P	P
Provide operational data on service usage	RA			CP	CP	P		
Funding for O&M tails	C	RA		C	C	C		
Follow Clinger-Cohen legal mandates		RA						
Resource Sponsor		RA	CP					

4.2.2. Demand Management

Demand Management is responsible for assessing expected usage levels of IT services, the need and impact to the business environment, and cost savings options (e.g., off-peak pricing, volume discounts, differentiated service, etc.) that will support USMC needs.

4.2.2.1. Objectives

Demand Management helps IT governance authorities understand the Marine Corps' FAMs and OPFORs requirements for IT services and how these requirements change over time. By varying the service provision or influencing customer demand, Demand Management helps to ensure the appropriate levels of service are always in place to meet current and anticipated future demand. Further, effective Demand Management will ensure that resources will not be wasted in supporting under-used or obsolete services.

4.2.2.2. Roles and Responsibilities

Table 4: Roles and Responsibilities Table for Demand Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for demand management	C	RA	C	C	C	C	C	C
Provide acquisition and technical inputs	P		RA					
Perform demand modeling and develop service options for estimated demand			RA					
Provide usage data for all provisioned IT services	RA			CP	CP	P	P	P

4.2.3. Service Portfolio Management

Service Portfolio Management is the process by which investments in different services across the enterprise are made to maximize the overall return on investment. It presents currently available services and service levels, future services and service levels, as well as archived services.

4.2.3.1. Objectives

Service Portfolio Management tracks the status of services throughout their lifecycle to identify when potential new services are required or existing services are no longer needed and should be retired. The Marine Corps will use the Service Portfolio as a framework from which to support Financial and Demand Management activities and establish and shape PoRs and their respective Service Catalogs to best support USMC IT service requirements.

4.2.3.2. Roles and Responsibilities

Table 5: Roles and Responsibilities Table for Service Portfolio Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Service Portfolio Management	C	RA	C	C	C	C	C	C
Establish service priorities and authorize resources	C	RA	C		CP			
Manage the SIPRNet service portfolio		RA			CP			
Provide acquisition and technical inputs	P	P	RA	P	P	P	P	P
Inventory services; validate portfolio data; provide cost/ROI data; and charter services			RA					
Provide operational prioritization of services	RA			C	CP			

4.3. SERVICE DESIGN

The objective of Service Design is to carry out Service Strategy by overseeing the efficient development and fielding of IT Services to meet identified requirements and mission needs. The roles and responsibilities of those involved in fielding Marine Corps capabilities the Service Design processes does not align with any single organization. MCSC is the owner of many of these processes as they fall within its acquisition mission. However, there is substantial involvement from HQMC Director C4 as the functional sponsor, MCNOSC as the technical advisor for operational requirements, the NetOps Community, and most importantly the MCEN SIPRNet user community the "customers".

4.3.1. Service Catalog Management

Service Catalog Management (SCM) provides a single source of consistent information on all of the agreed services that is widely available to those who are approved to access it. SCM is the process by which IT Services are offered and managed. The Service Catalog contains information about all live IT services, including those available for deployment. It is the only part of the Service Portfolio published to customers, and is used to support the delivery of IT services. The catalog serves the customer and user bases by providing them insight to service offerings so they can determine suitability to their operational needs and providing a vehicle through which to access.

4.3.1.1. Objectives

The service catalog will serve the Service Design (Acquisition) community as it provides a model to which they can design, provision, and programmatically manage Services. The catalog supports the Service Operations community as it is the basis for SLM negotiations with customers and users and the resultant SLA which will then drive execution of service processes and functions.

4.3.1.2. Roles and Responsibilities

Table 6: Roles and Responsibilities Table for SCM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for SCM	C	RA	C	C	C	C	C	C
Define offered services			RA					
Design SIPRNet services in support of SCM			RA					
Define services interfaces and/or dependencies between Service Catalog, Service Portfolio, etc.		A	R					
Provide performance and usage data for SIPRNet services	RA			CP	C			
Provide operational requirements	RA			CP				

4.3.2. Service Level Management (SLM)

SLM determines appropriate IT service targets, ensures that an agreed level of service is provided for all current IT services, and that future services are delivered to agreed targets. SLM is the process of negotiating, defining, measuring, managing, and improving the quality of IT services at an acceptable cost. SLM ensures that the IT services required by end users are continuously maintained and improved. This is accomplished through the establishment and enforcement of SLAs.

4.3.2.1. Objectives

As the USMC ITSM framework is constructed and matures, SLM is going to become both increasingly important and complex. In order to have an effective ITSM framework, we will need to develop the ITSM processes enabled by ITSM tools to manage capacity, availability, priorities/precedence, etc. to discriminate Service Levels and prioritize users and customers based on some military criteria - yet to be determined. In the near future, offered services and service level targets will be advertised in a service catalog.

4.3.2.2. Roles and Responsibilities

Table 7: Roles and Responsibilities Table for SLM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for SLM	C	RA	C	C	C	C	C	C
Design SIPRNet services in support of SLM	C		RA		C			
Develop SLA/OLA/service targets	CP		RA		C	C	C	
Authorize standard SLA/OLA/service targets	R	A						
Determine SLA/OLA/service targets breaches	RA			I	CP	P		
Identify SLA/OLA/service targets deficiencies	P		RA				C	C
Provide operational and service target requirements	P	RA	P	C	CP	P	C	P
Provide performance and usage data for SIPRNet services	RA		P	I	C			
Performs service monitor/reporting	RA		P	I	C			

4.3.3. Capacity Management

Capacity Management aims to consistently provide the required capacities needed to support IT Services and corresponding SLAs in a cost effective manner. It attempts to balance the need for sufficient room for growth/expansion while preventing the waste that goes with unnecessary excess capacity. It is a function of system/service design and as such is a process established between the acquisition community and the Service Operations (NetOps) community.

4.3.3.1. Objectives

Capacity Management is a process and design principle, and a key engineering task. Capacity Management for the SIPRNet will be a collaborative effort between the Acquisition community and Service Operations (NetOps) community. It is essential that all understand how capacity shortfalls in one service area potentially impact other levels of service. The NetOps community's role in Capacity Management is the production and review of data produced by various tools and other processes and development and provision of capacity forecasts. These forecasts will leverage change/action on a part of the respective Program Manager to ensure that system/service capacities are available in a manner that precludes negative impact to Service Operations/SLA. At the regional level of NetOps, Capacity Coordinators will be appointed to collect and assess data and forward to the Global Capacity Manager at the MCNOSC for final analysis and notification/RFC to the respective PoR.

4.3.3.2. Roles and Responsibilities

Table 8: Roles and Responsibilities Table for Capacity Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Capacity Management	C	RA	C	C	C	C	C	C
Process owner			RA					
Ensure process is followed			RA					
Design SIPRNet services in support of Capacity Management	C		RA		C			
Produce and maintain up-to-date SIPRNet capacity plan	C		RA					
Assist in the diagnosis of capacity-related problems	RA		P	I	P	P	C	
Ensure proactive cost-justifiable measures to improve performance			RA					
Perform capacity analysis	P		RA	I	P			
Assess current /future users and capabilities	C		RA		C	P		
Provide operational data on capacity usage	RA			I	CP			
Identify capacity problems	RA			I	CP			
Perform capacity forecasting	RA			I	CP			
Provide performance and usage data for SIPRNet services	RA			I	CP			

4.3.4. Availability Management

Availability Management is an element of design and is closely related to both Capacity and IT Service Continuity Management (ITSCM) processes and directly supports SLM. The role of Availability Management is to ensure all IT infrastructure, processes, tools, and roles are sufficient and appropriate to meet the service level targets for availability as advertised in the Service Catalog. Availability is determined by reliability, maintainability, serviceability, performance, and security factors, and is normally calculated as a percentage. The Capacity and Availability Management processes mutually inform one another, preferably in a proactive manner.

4.3.4.1. Objectives

Availability Management activities will be driven by service level target offerings from the Service Catalog and SLAs themselves. The USMC will develop a cross-project/program Availability Management framework that will support the development of a SIPRNet Availability Management process. As with Capacity Management, this process is very much federated in nature with both acquisition and operational involvement. The SIPRNet Availability Management process will be developed and evolve once the Service Catalog service level targets are known.

4.3.4.2. Roles and Responsibilities

Table 9: Roles and Responsibilities Table for Availability Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Availability Management	C	RA	C	C	C	C	C	C
Process owner			RA					
Ensure process is followed			RA					
Design SIPRNet services in support of Availability Management	C		RA		C			
Ensure IT Services support advertised Availability level within the Service Catalog			RA					
Create/maintain an SIPRNet Availability plan			RA					
Assess RFC impacts to Availability	R		A	I	CP			
Monitoring and reporting of Availability	RA			I	CP			
Proactive improvement of service availability and optimization of the IT infrastructure	CP		RA		CP	C		
Assist with investigation/diagnosis of incidents/problems which cause availability issues	RA		I	I	CP			
Provide operational data on service availability	RA			I	CP			
Identify availability problems	RA			I	CP			
Perform service failure analysis	RA			I	CP			
Provide performance and usage data for SIPRNet services	RA			I	CP			

4.3.5. IT Service Continuity Management (ITSCM)

ITSCM ensures that required IT services can be resumed within the timescales required to support operations. This process is responsible for managing risks to Service Operations/delivery and ensures that the service provider can always deliver minimum service levels as defined in service level targets and SLAs. This is done by reducing risk to the lowest affordable levels and providing for failover/recovery of IT Services and supporting Systems. ITSCM must be a major consideration at the time of design and implementation of IT Services. Redundancies to ensure High Availability/Continuity/Disaster Recovery (HA/C/DR) must be built into the design.

4.3.5.1. Objectives

ITSCM is a function of design and operational considerations. Anything beyond automatic failover will require knowledge and action by the NetOps community and these actions will be incorporated into operational instructions. For SIPRNet Services, ITSCM issues are being considered in the technical design. The MCNOSC will look to modify the current COOP to see if it requires adjustment to fully support.

4.3.5.2. Roles and Responsibilities

Table 10: Roles and Responsibilities Table for ITSCM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for ITSCM	C	RA	C	C	C	C	C	C
Approve service continuity thresholds	C	RA		C	C	C		C
Define service continuity thresholds with input from the customer	C		RAC	C	C	C	C	C
Process owner		RA						
Ensure process is followed		RA						
Service Continuity plan execution	RA			I	P			
Develop service continuity plans to maintain IT service continuity in support of USMC missions.	CP	RA	P	P	CP	CP	CP	CP
Perform impact/risk assessment and risk management to prevent disasters where cost justifiable and where practical	R		A	I	P	C	C	C
Assess potential service continuity issues, invoking the continuity plan as required.	RA			CP				
Perform post mortem reviews of service continuity tests/invocations and initiate corrective actions as required.	R		A	C	P			
Provide operational inputs to risk analysis	RA			C	CP	CP	C	C
Test service continuity plans	P	RA	P	P	CP	CP	CP	CP

4.3.6. Information Security Management (ISM)

ISM aligns IT security with DoD IA program requirements and operational requirements/objectives to ensure the security of the network, its services, and its applications. Information Security Management is the process through which IA (confidentiality, integrity, and availability of services, systems, and data) is integrated into the system design, allowing for interoperability with other security measures.

4.3.6.1. Objectives

Today, and for the foreseeable future, DoD Information Assurance Certification and Accreditation Process (DIACAP) will serve as the baseline Information Security Management process and will be supported by the Critical Infrastructure Protection (CIP) Program. PoRs will need to consider the network assurance architecture when designing systems and services to ensure compatibility and supportability.

4.3.6.2. Roles and Responsibilities

Table 11: Roles and Responsibilities Table for ISM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for ISM	C	RA	C	C	C	C	C	C
Process Owner		RA						
Ensure process is followed		RA						
Produce, maintain, distribute, and enforce IA/IT security policies	C	RA		I				
Design SIPRNet services			RA					
Document current/future requirements	C	RA	CP	C	C			
Certify services in accordance with the DIACAP	P	RA	P					
Implement security controls in services	P		RA	I	P			
Proactively improve security controls	R		A	I	CP			
Provide input to current/future requirements	RA			CP	CP	P	C	C
Provide performance and usage data for SIPRNet services	RA			I	CP			
Monitor for unauthorized activity	RA			I	CP			
Report unauthorized or suspicious activity	RA	P	P	CP	CP	P	CP	CP
Initiate security incident response	RA	P	P	P	P	P	P	P
Document breaches/incidents	RA	P	P	CP	CP	P	P	P
Assignment of MAC levels	R	A		I	I	I	R	I
Develop policies, guidance, and establish	C	RA	C	C	C	C	C	C

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
responsibilities for Certification and Accreditation (C&A)								
C&A review	RA	CP	CP					
Ensure appropriate network certification and accreditations are completed	R	I	A	CP	CP		C	

4.3.6.3. Mission Criticality Assessments

The Marine Corps is required to assign a Mission Assurance Category (MAC) to their information systems in accordance with DoD Instruction 8500.2 (reference W). The MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories:

- **MAC I**: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

- **MAC II**: Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

- **MAC III**: Systems handling information that is necessary for the conduct of day-to-day business, but do not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices. (DoDI 8500.2 reference Y)

While MAC determination is provided by the system owner and documented in the systems accreditation, all RNOSCs must maintain and keep ready access to the MAC levels of all SIPRNet information systems in their region. Additionally, as new systems are brought online, RNOSCs should ensure a system owner determination is made as to their mission category. In doing this, operational impact assessments can be conducted quickly in responding to a SIPRNet event or incident. Caution: Care should be taken in correctly assigning MAC levels to information systems. The system MAC levels may determine reporting time frames and whether the event or incident is a Commanders Critical Information Requirements (CCIR).

4.3.6.4. Certification and Accreditation (C&A)

It is Marine Corps policy that all information systems shall be certified and accredited through an enterprise process for identifying, implementing, and managing IA capabilities and services. The Marine Corps shall establish and use a service enterprise decision structure for the Marine Corps Certification and Accreditation Process (MCCAP). MCCAP shall support the transition of information systems to GIG standards and a net-centric environment while enabling assured information sharing by:

- Providing a standard C&A approach
- Managing and disseminating service enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting. These standards and guidelines can be accessed at: https://hqdod.hqmc.usmc.mil/IA/Pages/Orders.asp
- Accommodating diverse information systems in a dynamic environment

All Marine Corps owned, controlled, or supported information systems shall be under the governance of the Marine Corps IA Program (MCIAP) and fall under the MCNOSC CND service provider. The MCIAP shall be the primary mechanism for ensuring enterprise visibility and synchronization of the MCCAP.

For all Marine Corps information systems requiring C&A, the responsible PM or Information Assurance Manager (IAM) shall create a DIACAP package using the specified automated support tool for the MCCAP. This enables PMs and IAMs within the Marine Corps to determine the scope and state of all IA activities within the SIPRNet in order to identify IA requirements develop policy, manage and train personnel, and make decisions concerning acquisition, IA resources, and programming.

All Marine Corps information systems shall be implemented using the baseline DoD IA controls in accordance with DoDI 8500.2 for unclassified, sensitive, and collateral classified information. The baseline DoD IA controls may be augmented, but not reduced, if required to address localized threats or vulnerabilities.

4.3.6.4.1. Objectives

The C&A process will ensure adequate security measures are in place to protect the information that resides on Marine Corps systems. This process is applicable to all Marine Corps systems under development and those already in operation. In addition, Federal laws and regulations require Federal agencies to perform C&A activities at least every three years or when a major change has been made to the system. To meet the C&A requirements mandated in Federal laws, the Marine Corps has outlined C&A requirements in Marine Corps Enterprise Information Assurance Directive 018, MCCAP. Therefore, organizations, commands, bases, and stations within the Marine Corps are required to adhere to Marine Corps-wide policy.

The C&A process will achieve the following:

- Validate security requirements established for a system or network
- Examine implemented safeguards to determine if they satisfy Marine Corps' security requirements and identifies any inadequacies
- Obtain management approval to authorize initial or continued operation of the system or network.

4.3.7. Supplier Management

Supplier Management is the process through which we ensure that supplier contracts effectively meet the needs of IT services and the business areas which they support.

4.3.7.1. Objectives

Today, Supplier Management is largely done within PoRs. However, for those legacy IT services and systems not yet supported by a PoR, the MCNOSC, and other operational organizations, conduct Supplier Management in concert with MCSC. As the Marine Corps transitions IT services to PoRs, the enterprise approaches the state presented in Table 12 below. As reliance on vendor support is likely throughout many areas of the SIPRNet solution, this process will grow in importance.

The key to effective Supplier Management is well-written performance-based services contracts, but this depends fundamentally on the ability to measure and baseline performance throughout the enterprise. By accurately measuring Key Performance Indicator (KPIs) and other metrics, consist with other geographic locations, operational organizations allow the development of Performance Work Statements (PWS) that describe an improvement in measurement over time. These improvements are made enforceable to vendors by tying award fees to measured performance. However, vendors will not agree to such contracts unless performance metrics are also described for the government to meet. Good measurement also ensures that these agreements are upheld in a verifiable way.

Supplier Management has a critical interface with SLM wherever SLAs depend on vendor performance. Underpinning Contracts (UC) must be designed to enable SLAs to be met, because despite vendor performance, the enterprise is accountable for meeting its SLAs to end users. In contrast, Service Level Management must communicate with Supplier Management if a change to a SLA is proposed. Such a change may have costly effects on existing and future contracts. These two processes are linked by the fact that contracts and SLAs are CIs, subject to Change Management. RFCs must be signed off on both sides.

4.3.7.2. Roles and Responsibilities

Table 12: Roles and Responsibilities Table for Supplier Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Supplier Management	C	RA	C	C	C	C	C	C
Negotiate and manage under pinning contracts			RA					
Maintain supplier policy and supporting supplier and contract database			RA					
Monitor supplier performance	P		RA	P	CP	P	P	P

4.4. SERVICE TRANSITION

The objective of Service Transition is to plan and manage resources to successfully add a new service to or change an existing IT service in the Marine Corps SIPRNet environment with minimal unpredicted impact to this critical operational network. This will maximize end-user satisfaction. As with Service Design, the Service Transition processes do not and cannot always align with any single organizational entity. Process ownership varies at this intermediary step in the service lifecycle as a result of the service or capability transitioning from the Service Design to Service Operation stages. Significant involvement from HQMC C4, MCSC, and MCNOSC occurs in nearly all of them – HQMC C4 from a policy and guidance perspective, MCSC from a design accountability perspective, and MCNOSC from an implementation perspective.

4.4.1. Change Management

Change Management are the processes that ensure changes to IT services or service Configuration Items (CI) are evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner before being deployed to the operational environment. The objective of Change Management is to mitigate risk to services by ensuring that all effected changes (adds, removals, modifications) minimize impact to IT services and the business processes they support. There are typically three types of changes – standard, normal, and emergency. Standard changes are typically

small changes pre-approved by Change Management that are low risk, frequently occurring, and low cost. Typical standard changes include: a request to change a password, a request to install an additional software application onto a particular workstation, and a request to relocate some items of desktop equipment. Normal changes are typically new or non-standard changes for which implementation time allows for handling via the full change management process. Emergency changes are typically a change that must be introduced as soon as possible and normally have an abbreviated change management process. Typical emergency changes include implementation of a security patch required for a major incident or a change required to restore service.

4.4.1.1. Objectives

Due to the nature of the USMC acquisition process and the authorities vested in its PMs, Change Management is a process that is largely resident in the acquisition community but which requires considerable involvement of the Service Operations and IT Security Management (in particular the USMC DIACAP process) communities. A Change Management framework will be proposed by HQMC Director C4. Change Managers should be appointed within each PoR and at the MCNOSC. Change Coordinators should be established within each region and could be used as Change Managers for regionally/locally owned IT services. The ITSM tool suite will be configured to support a cross-PoR Change Management. MCNOSC will exercise full Change Management and Change Advisory Board authorities for operational level changes and will record, classify, and comment on PoR RFCs before passing-on to the Program Change Manager. These actions will take place on Change Records within the ITSM tool suite. Change Management/CAB function will be developed within the SONIC PoR to execute PM authorities.

4.4.1.2. Roles and Responsibilities

The following table contains roles and responsibilities that are pending further definition through the ITSM effort.

Table 13: Roles and Responsibilities Table for Change Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Change Management	C	RA	C	C	C	C	C	C
Comply with DIACAP requirements for changes that affect the security posture of the network	R		A	CP	P			
Obtain contractor and vendor support, as required			RA					
Develop implementation plan and change schedule	R		A	CP	CP	P	C	
Assess whether DIACAP Certification and	R		A	CP	P			

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Accreditation is required								
Direct required validation testing	R		A	I	CP			
Coordinate Release, Build, Test, and Implementation	R		A	I	CP	P		
Review/close RFC	R		A	CP	P			
Conduct trend analysis	R		A	I	CP			
Generate Request For Change (RFC)	R	A	P	P	P	P	P	P

4.4.2. Release and Deployment Management

Release and Deployment Management (RDM) processes deploy both new services and changes to existing services into the enterprise and establish effective use of these services in support of operations. It is the process through which changes to the IT environment are actually effected (released/deployed into the production environment). Approved Changes are assembled into "Releases" (from Project Management) and subsequently deployed in a disciplined and scheduled fashion. A release consists of hardware, software, peripheral items, technical instructions, procedures, and anything else required to deliver the approved change as well as the knowledge and skills required to operate the new/updated service.

4.4.2.1. Objectives

The goals of RDM are to ensure that deployment/release plans are thorough, supportable, and minimize impact to current operations. Release deployments can be executed via several approaches—in its entirety or incremental/ phased, pushed vs. pulled, and automated vs. manual. Any and all of these could be used in combination as long as it represents the most effective and efficient method for achieving the desired results.

RDM requires process and build managers. As with Change Management, this requires substantial activity/engagement on the part of both Service Design (USMC acquisition community) and Service Operations (NetOps community). It is envisioned that each IT service PoR will require a Release and Build Manager to ensure that changes to PoR services/systems meet the approved requirements and are appropriately bundled and scheduled. The MCNOSC will have a Release and Deployment Manager to coordinate the release deployment between the PoR, IT operations personnel, and the USMC business process owners (customers). Finally, there will be Release Coordinators assigned within regional NetOps to coordinate release deployments with the MCNOSC and respective PoRs. These Release Coordinators will likely serve as the Release and Deployment Managers for regional/local IT services and infrastructure.

4.4.2.2. Roles and Responsibilities

Table 14: Roles and Responsibilities Table for RDM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for RDM	C	RA	C	C	C	C	C	C
Establish RDM framework	CP	C	RA	C				
Conduct periodic audits of releases	R	A	I	C				
Assess release management framework for needed modification	R	A	I	C				
Modify Release and Deployment framework	C	RA	C	C				
Assign responsibilities to organizations		RA						
Process owner			RA					
Develop Process	C		RA	C	C			
Ensure process is followed			RA					
Develop Release Plan [in coordination with Change Management, SKMS, and SACM processes]	CP		RA	I	CP			
Approve Release Plan	CP		RA	C	C			
Build and Configure Release			RA					
Develop Roll-out/Back-out Plan	R		A		CP			
Approve Roll-out/Back-out Plan	CP		RA	I				
Implement (Deploy) the Release	RA		I		P	P		
Conduct Operational Testing	R		A		P	P		
Provide/conduct Training	P		RA		P	P		
Accept Release	RA		I	P				
Execute Back-Out Plan (if required)	RA		I		P	P		

4.4.3. Service Asset and Configuration Management (SACM)

The process through which service assets are managed through their lifecycles (Asset Management) and that approved configuration of the IT infrastructure is maintained, documented and validated. SACM within the ITILv3 framework is concerned with the definition, control of, and relationship between CIs and services/SLAs/customers. A CI is any asset to which change must be approved through the Change Management process due to its role in the delivery of an IT Service. SACM is instrumental to ensuring the integrity of assets and CIs, thereby leading to a reduction of unapproved changes to the IT Service Infrastructure as well as the resultant incidents and problems. This results in more reliable IT Services, better compliance with SLAs, more satisfied customers, and greater real and perceived value of IT to the business community.

4.4.3.1. Objectives

Instrumental to SACM is the CMS. CMS consists of the Configuration Management Data Base (CMDB)[1], Asset DB, and the Definitive Media Library (DML). The CMS will contain detailed configuration data for each CI, appropriate details associated for each Asset, and all media required to support IT services. The CMS will be constructed within the ITSM Tool set and should be a federated system that supports the needs of both the acquisition and NetOps communities at all levels. It is envisioned that there will be Asset and Configuration Managers in the Acquisition community at the PoR level as well as in the MCNOSC. There will be a need for an Asset and Configuration Coordinator within each NetOps region to coordinate on issues with the MCNOSC.

4.4.3.2. Roles and Responsibilities

Table 15: Roles and Responsibilities Table for SACM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for SACM	C	RA	C	C	C	C	C	C
Develop Configuration Mgmt Framework	P	A	R	C	C			
Assess Configuration Mgmt Framework	P	A	R	C	C			
Modify Configuration Mgmt Framework	P	A	R	C	C			
Assign responsibilities to organizations		RA						
Maintain SIPRNet Configuration Management System	RA		P	P	P			
Maintain SIPRNet CMDB Data to include historical, current, and planned configurations for all CIs	RA		P	I	I			
Process owner	R		A					
Ensure process is followed	R		A	P	P			
Develop Configuration Mgmt Methodology/Process	R		A	P	P	C	C	
Implement Configuration Management	R		A	P	P			
Implement CMDB	R		A	P	P			
Develop Linkage to Asset Discovery Tool	R		A		C	C		
Develop Configuration Management Reporting	R		A	P	P			
Recommend CIs	R		A	P	P			
Approve CIs	R		A	P	P			
Develop Configuration Interfaces and Controls	R		A	P	P			
Document Configuration	R		A	P	P			
Document approved Configuration Change	R		A					
Monitor approved Configuration changes; and implement minor Configuration changes	RA			P	P			
Perform Configuration audits and identify unauthorized Configurations	RA		I	P	P	P		

[1] Pending outcome of E-ITSM, the CMDB may be a federated group of databases.

4.4.4. Knowledge Management

Knowledge Management (KM) is the process through which all relevant, accurate, reliable, and secure data and information about the IT Service Infrastructure and all supporting processes and functions are gathered, organized, stored, maintained, and made available. KM includes document, record, e-mail, digital asset, and web content management.

4.4.4.1. Objectives

Quality service delivery is dependent upon effective response to operational circumstances. To be effective in response, parties involved in the provision of IT services through the ITSM framework must have timely and directed access to accurate and relevant information.

4.4.4.2. Roles and Responsibilities

Table 16: Roles and Responsibilities Table for KM

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for KM	C	RA	C	C	C	C	C	C
Develop a KM framework	R	C	A	C	C	C	C	C
Assess the KM framework	R	P	A	P				
Modify the KM framework	R	I	A	I	I			I
Process owner			RA					
Ensure process is followed	R		A	I	P	I		I
Capture and store information and data	R		A	I	P	I		I
Categorization/Taxonomy	R		A	I	P			
Indexing	R		A	I	P			
Manage information	R		A	I	P			
Business process management / workflow	R		A	I	P			
Publishing content	R		A	I	P			
Provide content input	R	P	A	P	P	P	C	C
Access content	R	P	A	P	P	P	C	C
Change recommendation	R	P	A	P	CP	P		C
Digital rights management/access control	R		A	C	P			C

4.5. IT SERVICE OPERATIONS

The objective of Service Operation is the day-to-day management of the technology used to deliver and support IT services, as well as the coordination and conduct of activities, processes, and functions required to deliver and manage services at agreed SLAs for USMC end-users and customers. These activities include, but are not limited to, monitoring performance, gathering data, and analyzing metrics on the SIPRNet and its associated infrastructure, hardware, and applications. MCNOSC is the owner for Service Operation processes. Execution of these operational activities occurs though several groups of skilled personnel within the Service Desk, Technical Management, IT Operations Management, and Application Management functions. At the core of its Service Operations, the USMC maintains a ESD managed by the MCNOSC and supported by technical and application specialists/touch labor within the regions. Technical Management provides the detailed technical skills and resources to supporting the ongoing operation of the IT Infrastructure. IT Operations Management executes the daily operational activities needed to manage the IT infrastructure in the delivery of IT Services. Application Management provides the detailed skills and resources for managing applications throughout their lifecycle, predominantly through MCEITS.

4.5.1. Service Desk/Request Fulfillment

The service desk is a functional entity made up of a dedicated number of staff responsible for coordinating and carrying out the activities and processes required to deliver and manage services at agreed levels for supported users.

4.5.1.1. Objectives

The SIPRNet service desk will be implemented at an enterprise level in order to better support the overall garrison network transition and realignment, implementation of ITSM processes and NetCOP toolsets.

The ESD, in its end-state, will coordinate actions across all IT organizations, and keep status updates, resolution and communication flowing back and forth. It will be responsive and have the ability to oversee the entire enterprise. Most importantly, it will need to act upon any degradation of services that could cause major outages before they happen.

Eventually, the enterprise service desk will support all user issues, including fixing technical faults, logging and categorizing incidents or events, responding to a service request or answering a query, and coordinating "standard" changes[1]. Specifically, the ESD will encompass the following Service Operations processes, detailed in later sections:

- Incident Management
- Access Management
- Problem Management
- Request Fulfillment

4.5.1.2. Transition

During the transition, local support procedures will be used as enterprise processes are being developed. The focus of effort will be on training and hiring touch labor support personnel at the B/S G6s, as well as hiring adequate MITSC staff to support situational awareness, prioritization, deployed support operations, and escalation procedures. The MITSCs will manage their end-user resources and manage all touch labor responding to end-user issues within their regions. The respective RNOSC is responsible for management oversight of these MITSCs.

Coordination and MCNOSC hiring actions will begin standing up the primary enterprise service desk at Kansas City, Missouri, with Initial Operating Capability (IOC) during

Fourth Quarter Fiscal Year 2010 (4QFY10). IOC capability for an alternate enterprise service desk (specific location under evaluation) is currently being explored. Full Operational Capability (FOC) of the alternate enterprise service desk will take place once all required ITSM processes have been fielded and the requisite NetCOP tools have been procured and installed.

FOC for the primary enterprise service desk will occur when all SIPRNet and NIPRNet domains and users have been transitioned to this support structure.

4.5.1.3. Enterprise Service Desk (ESD)

The ESD will be provided at the enterprise level as a service to the entire Marine Corps. ADCON of the enterprise service desk will be by the Director C4 and be delegated to the Commanding Officer, MCNOSC. Staff is available 24x7 to receive user-submitted requests and respond to incidents. Surge support can be preplanned as required.

All non-VIP service requests and incident reports go directly to the Enterprise Service Desk. ESD personnel log the request/incident in the trouble ticket management system and provide first line investigation/diagnosis/response through phone or remote access. If the request/incident is resolved over the phone, user satisfaction is verified and the request/incident is closed. If the request/incident is not able to be resolved immediately,

[1] Refer to section 4.4.1 (Change Management) for more information on standard changes.

the service desk is authorized to and will assign the request/incident to the appropriate USMC organization for action. The assigned local technician will fully investigate the resolution/answer. If a solution is known, the local technician will attempt to resolve the matter in person. If the solution cannot be identified, the local technician will escalate the incident/request to their MITSC through the trouble ticket management system, but will remain engaged until the issue is resolved. The MITSC will escalate the ticket to MCNOSC as required. The assigned Enterprise Service Desk technician is responsible for coordinating status with the organizations touch labor or MCNOSC, and ultimately keeping the user apprised of the status. Enterprise Service Desk staff must always track the request until verification of user satisfaction and request/incident closure. User and customer interaction with the technical staff should only be initiated through the service desk. Technicians may directly engage the user to solicit more information or coordinate resolution. An alternate ESD will be maintained to provide continuity and redundancy.

Figure 18 graphically depicts the ticket flows at the enterprise, regional, and local levels.

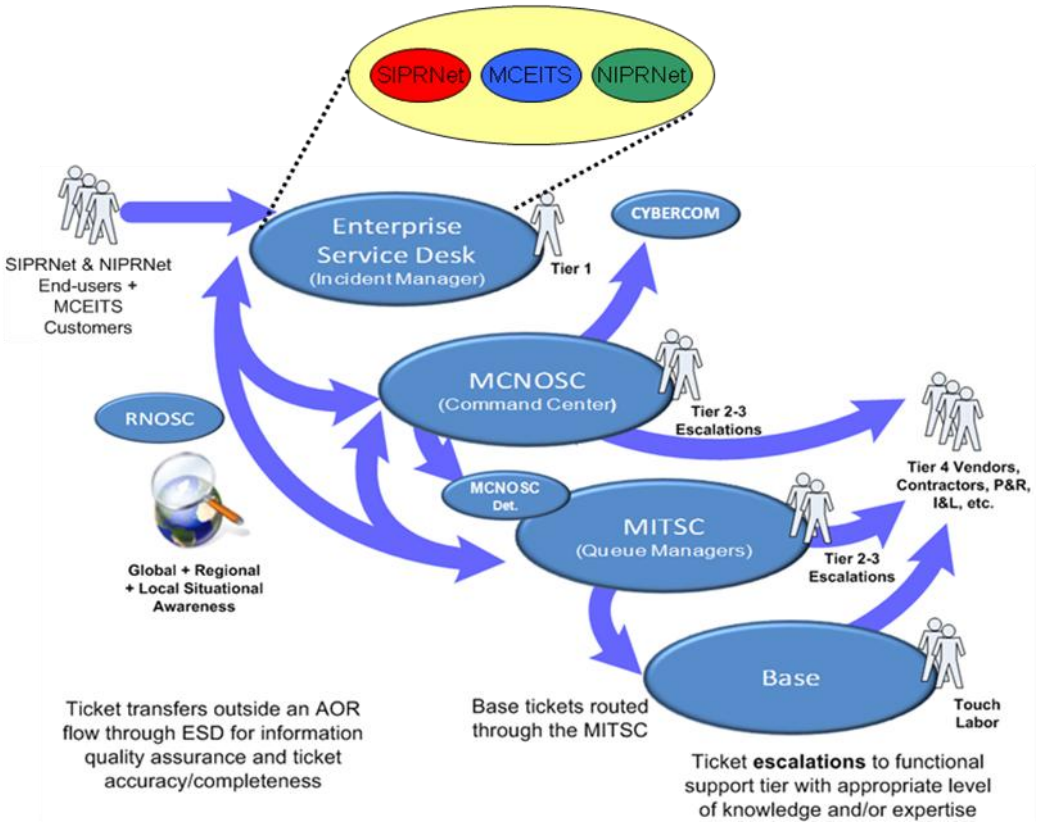

Figure 18: Ticket Flows

4.5.1.4. Very Important Persons (VIPs)

For the purposes of the SIPRNet, Very Important Persons (VIPs) are defined across the Marine Corps SIPRNet as 'General Officers or their Senior Executive Service (SES) civilian equivalents. Based upon the total number of VIPs within a particular region, a MITSC is allocated additional manpower resources. This extra touch labor is meant to provide an improved response time (i.e., more stringent SLA) for VIP service requests in the garrison environment. MITSCs are authorized to locally designate other individuals as VIPs, however services for non-General Officer/SES VIPs are provided at the MITSCs own expense and with an obligation to still meet SLAs for non-VIP users. From an ESD perspective, locally-designated VIPs are not authorized the more stringent SLAs as is the case for General Officers or SES. MITSCs may locally adjust prioritization and technician assignments within their trouble ticket management system queue to provide improved response time to these locally-designated VIPs. However, non-VIP users must still receive service within agreed SLAs.

4.5.1.5. Super Users

A pre-designated person(s) authorized to assume temporary elevated access controls and authorizations for the purpose of resolving high priority incidents or incidents involving VIPs. These elevated rights are granted once the super-user opens a ticket with the ESD and is validated as a pre-defined Super-User. The ESD Analyst/ticket owner will be responsible for monitoring the resolution of the problem and rescinding the elevated rights once the incident has been resolved.

4.5.1.6. Internal IT Support

The ESD concept described above does not “prohibit” organizations from maintaining their own internal IT support in particular in support of VIPs or those locally designated as VIPs. However, this does not alleviate the mandatory requirement for all IT support requests to ultimately go through the ESD for ticket logging – even if accomplished after the service or support has been provided. It is also important to note that resourcing of any IT support (service desk or touch labor) outside the ESD concept is at the local unit’s expense. The MITSC is allowed to delegate permission to subordinate G/S6 as long as the IT support staff is following enterprise practices and meets required certification and training standards.

4.5.1.7. Roles and Responsibilities

Table 17: Roles and Responsibilities Table for Service Desk/ Request Fulfillment

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for ESD/Request Fulfillment	C	RA	C	C	C	C	C	C
Functional owner for service desk structure, toolset and parameters	RA							
Inform higher headquarters of NetOps situations/issues per established CCIRs	RA	I	I	I	I	I	I	I
Manage the ESD	RA							
Act as a conduit to vendor support	RA		P	I	P	P		
Coordinate actions across the IT organization to meet user requirements	R	A	CP	CP	CP	CP		CP
Manage end-user resources and manage all touch labor responding to end-user issues within the region				I	RA	P		
Provide for enterprise tracking of issues, incidents, and service requests while maintaining full situational awareness at all levels	RA							
Ensure ESD supports Incident, Event, Request Fulfillment, and Access Mgmt processes as required	RA							
Provide reports in support of ITIL Process Managers as required	RA			CP	CP	CP		
Provide first line investigation/diagnosis/response (phone or remote access)	RA							CP
Logging and categorization of Incidents, Service Requests and standard changes	RA							
Coordinate with Incident/Event/Problem Management process, as required	RA							
Verify user satisfaction with resolution	RA				P	P		P
Ensure closure once user satisfaction verified	RA							

4.5.2. Event Management

Event Management is the process through which events are managed throughout their entire lifecycle. An event represents any change of state which has significance for the management/operation of a CI or service. Events often come to light through alerts or notification from either a monitoring tool or the CI itself and usually require some level of engagement on the part of Technical Management personnel. If the event results in some form of unplanned interruption of an IT Service or impacts a CI, it would be reported and recorded as an incident. SIPRNet Event Management will be conformed to that for all of NetOps services.

4.5.2.1. Objectives

Event Managers will be appointed at the global and regional levels. Events will be recorded, reported, and assessed and all actions taken in reaction to an event will be recorded in an event log. Event Managers at each level of NetOps will coordinate on those events with their counterparts at the different NetOps levels as required for proactive notification. The event log should be a federated tool that is available to all Event Managers for review and evaluation. Event Managers should be sharing their analysis with their counterparts whenever it is believed to benefit overall IT Service operations performance.

4.5.2.2. Roles and Responsibilities

Table 18: Roles and Responsibilities Table for Event Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Event Management	C	RA	C	C	C	C	C	C
Inform higher headquarters of NetOps Events per established CCIR	RA			P	P			
Process owner	RA							
Define points of entry for network Event Mgmt	RA				C			
Define Models	RA							
Identify Steps Taken to Handle Event	RA							
Identify Chronology of those Steps	RA							
Identify responsibility assignments for each step	RA							
Establish Timelines and Thresholds for completion of each action	RA							
Define Escalation Procedures	RA							
Define necessary evidence preservation activities	RA							
Define "Major" Event	RA							
Ensure process is followed	RA			I	P			
Identify event	RA				P			
Log	RA				P			
Define processes, procedures and tools to Log	RA							
Define format and content of Log entry	RA							
Perform Initial Categorization	RA				P			
Perform Prioritization	RA				P			
Perform Initial Diagnosis	RA				P			
Coordinate with Service Desk and Incident Mgmt Manager as required	RA				P			
Evaluate for local, regional or global impact	RA			I	P			

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Perform reporting and escalation, as required for type of impact (MITSC-local; RNOSC-regional; USCYBERCOM/MCNOSC-global)	RA			I	P			
Perform Investigation and Diagnosis	RA				P			
Perform Resolution and Recovery	RA				P			
Rebuild/restore systems following an IA event	RA				P			
Perform Closure	RA				CP			
Review/Correct Categorization	RA				CP			
Complete Documentation	RA				P			
Determine probability of Event recurrence	RA			I	CP			
Formally Close the Event	RA			I	CP			

4.5.3. Incident Management

An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident. Incident Management is the process for dealing with all incidents; this can include failures, questions or queries reported by the users, by technical staff, or automatically detected and reported by event monitoring tools. Incident Management processes restore normal service operation as quickly as possible and minimize the adverse impact on operations due to an incident.

4.5.3.1. Objectives

The objective of Incident Management is to return to the normal service level, as defined by the SLAs, as soon as possible and with the smallest possible impact to Marine Corps customer business processes and their end users. Incidents can be reported by any user, technician, or manager of IT services. Incidents will be reported to the enterprise service desk for initial recording and troubleshooting. Incidents will be escalated up the technical support tiers as mandated by SLA. The enterprise Trouble Ticketing System (TTS) will be designed to permit this flow of incident trouble tickets. Incident Managers will be appointed at each MITSC and at the MCNOSC. Incident Managers are responsible for the execution of their respective portion of the enterprise Incident Management framework and will communicate and coordinate with their counterparts on incidents or the process itself when required/beneficial.

4.5.3.2. Roles and Responsibilities

Table 19: Roles and Responsibilities Table for Incident Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Incident Management	C	RA	C	C	C	C	C	C
Incident identification	RA			P	P	P	P	P
Inform higher headquarters of NetOps Incidents per established CCIR	RA			C	P			
Act as a conduit to vendor support	RA		P	I	P	P		
Process owner	RA							
Define Models	RA			C	P			
Identify Steps Taken to Handle Incident	RA			C	P			
Identify responsibility assignments for each step	RA			C	P			
Establish Timelines and Thresholds for completion of each action	RA							
Define Escalation Procedures	RA							
Refine Models with "Major" criteria	RA	I	P	P	P	P		
Ensure process is followed	RA				P			
Report Incident	RA	P	P	P	P	P	P	P
Log	RA				P			
Define processes, procedures and tools to Log	RA				CP			
Define format and content of Log entry	RA				C			
Perform Initial Categorization	RA			C	C	C		
Perform Prioritization	RA			C	C	C		
Perform Initial Diagnosis	RA				P			
Coordinate with Service Desk, Event Mgr, and Problem Mgr as required	RA				P			
Evaluate for local, regional or global impact	RA			C	P			
Perform reporting and escalation, as required for type of impact (MITSC-local; RNOSC-regional; USCYBERCOM/MCNOSC-global)	RA			C	P	P		
Perform Investigation and Diagnosis	RA				P			
Perform Resolution and Recovery	RA				P			
Rebuild/restore systems following an IA incident	RA				P			
Perform Closure	RA				P	I		
Review/Correct Categorization	RA				P			
Solicit customer feedback (i.e. user satisfaction survey)	RA				P			
Complete Documentation	RA				P			
Determine probability of recurrence					RA			
Formally Close the Incident	RA			I	P			
Maintain Alarm surveillance	RA				P			

4.5.4. Problem Management

Problem Management processes identify problems and their root cause to drive changes to the service/infrastructure that will eliminate recurring incidents.

4.5.4.1. Objectives

Problem Management is the process through which problems are managed. A problem is something that is the cause of one or more incidents but for which the cause is not known. The overarching goal of Problem Management is to minimize the impact of or prevent incidents associated with IT services. The objective of Problem Management is to discover the root cause of a problem so appropriate action can be taken to preclude similar incidents in the future. Problems may be sourced to CIs, personnel (training), or procedures. Ideally, Problem Management is performed as proactively as possible. This is done through the analysis of Event and Incident Records as well as the data produced from other process areas (Capacity Management, Availability Management, Configuration Management, etc.). Each problem will have a record established that will capture all details and actions taken regarding the problem.

Problem Managers will be appointed at the global, regional, and local levels. At the regional level, the Problem Manager may exist either at the RNOSC or MITSC but the MITSC is the preferred location due to the proximity and greater access and visibility to the technical infrastructure (CIs) and operations. As with Incident Management, the NetOps community requires at a minimum, a confederated Problem Management process and supporting tool set (Record Log) with visibility by all parties. Problems will be identified, logged, and worked for resolution at the appropriate NetOps level. Problem Managers should immediately alert their counterparts at the other levels of any Problem that may impact them or require their support in root cause discovery.

4.5.4.2. Roles and Responsibilities

Table 20: Roles and Responsibilities Table for Problem Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Problem Management	C	RA	C	C	C	C	C	C
Inform higher headquarters of NetOps situations/issues per established CCIR	RA			C	P			C
Act as a conduit to vendor support	RA		P	I	P	P		
Operate and manage SIPRNet services	RA			C	P			
Process owner	RA							
Define models	RA							
Identify steps taken to handle problem	RA			C	P			P
Identify responsibility assignments for each step	RA			C	P			P
Establish timelines and thresholds for completion of each action	RA			I	C			C
Define escalation procedures	RA			I	C			C
Define "Major" problems	RA							
Refine Models with "Major" criteria	RA							
Ensure process is followed	RA			I	P			
Log	RA			I	P			
Define processes, procedures and tools to Log	RA				CP			
Define format and content of Log entry	RA				C			
Perform initial categorization	RA			I	P	P		P
Perform prioritization	RA			I	P	C		C
Approve prioritization	RA			P	P			
Perform investigation and diagnosis (Provide fault localization service)	RA			I	P			P
Coordinate with Incident, Event, and Change Mgrs as required	RA			I	P			P
Evaluate for local, regional or global impact	RA			C	P			P
Perform reporting and escalation, as required for type of impact (MITSC-local; RNOSC-regional; USCYBERCOM/MCNOSC-global)	RA			C	P			C
Perform Closure then submit RFC	RA			I	P			
Review/correct categorization	RA			P				
Complete documentation/update CMDB	RA			I	P			
Determine probability of recurrence	RA			I	P			

4.5.5. Access Management

Access Management is the process through which users are granted access to IT services, systems, CIs, or data while preventing access to non-authorized users.

4.5.5.1. Objectives

Access Management provides the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in IT Security and Availability Management. This process is a major component of IA as it protects confidentiality, availability, and integrity of assets, services, and data by ensuring that only authorized users/personnel are permitted access rights and are provided the ability to modify. While this process is largely carried out by IT Operations or ESD personnel, it is wholly dependent on the Identity Management mechanisms and architecture that are provided through the Service Design processes and that are incorporated into technical solutions (Single Sign-on, CAC, PKI, etc.).

DD Form 2875 System Access Authorization Request (SAAR) is the means of obtaining SIPRNet Access. [DoD Directive 8500.01E authorizes collection of this information. Executive Order 10450, 9397; and 18 United States Code (USC) 1030, The Computer Fraud and Abuse Act.] The process is as follows:
1. The user completes the online Personally Identifiable Information (PII) training and provides the printed certificate to the Information Assurance Officer. This training is required annually (calendar year) and can be found at the following NIPRNet website: http://iase.disa.mil/eta/pii/pii_module/pii_module/module.htm
2. The user completes the online Information Assurance Awareness (IAA) training and provides the printed certificate to the Information Assurance Officer. This training is required annually (calendar year) and can be found at the following NIPRNet website: http://iase.disa.mil/eta/iaav8/iaav8/index.htm
3. The user initiates the form and signs endorsements as to completion of annual (or refresh) training requirements.
4. The requesting user's supervisor or sponsor then endorses the need for SIPRNet Access.
5. This need is further validated by the Information Assurance Officer.
6. The Command Security Manager then endorses individual clearance and investigation levels to ensure the user is cleared for requested access. Completed SAAR Forms are maintained within the user's location.
7. MITSC or designated G6/S6 representative than contacts the ESD and submits a trouble ticket requesting SIPRNet access on behalf of the user.
8. Upon receiving the trouble ticket, a network administrator at the MITSC or delegated B/S prepares an account and the user is provided with his initial password upon positive identification.

The ESD and NetOps community will have the authority to both process and respond to user MCEN Garrison SIPRNet service requests. Initially, the global NetOps role in this process will likely entail the provisioning of operational direction and policy (from HQMC Director C4).

4.5.5.2. Roles and Responsibilities

Table 21: Roles and Responsibilities Table for Access Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for Access Management	C	RA	C	C	C	C	C	C
Process owner		RA						
Ensure process is followed	R	A		CP	P	P		P
Define Access Request Process	P	RA	C				I	I
Perform User Verification	RA			I	P	P	C	P
Enforce Access Control Rights	RA			CP	P	P	C	I
Log and Track Access	RA			I	P	P	C	I
Remove or Restrict Rights at enterprise level	RA			I	I	I	C	I
Remove or Restrict Rights at regional level	RA			I	P	I	C	I
Remove or Restrict Rights at local level	RA			I	P	P	C	P
Verify identity;	RA			I	P	P	P	P
Grant access privileges to services and data aligned with approved user access requirements and need to know	RA			CP	P	P	PC	PC
Perform logging and tracking of service access	RA			I	P			
Remove or restrict access when appropriate	RA			I	P	P	C	P

4.6. CONTINUAL SERVICE IMPROVEMENT (CSI)

CSI is a process designed to maintain the quality of all delivered SIPRNet IT services and the overall health of ITSM. It is accomplished through learning and improving on the processes involved in each phase of the ITIL Service Lifecycle and continually aligning IT services with Marine Corps mission needs and monitoring the maturity of these processes. These continual improvements help to ensure the effectiveness and efficiency of each phase. CSI includes performing internal audits, gathering information on customer satisfaction, making recommendations, and reviewing the service and deliverables for relevance and for further improvement opportunities.

4.6.1. Objectives

Reviewing and improving on aspects of each ITIL Service Lifecycle phase. Applying activities that improve overall IT service quality, as well as ITSM processes. Ensuring customer satisfaction while maintaining cost effectiveness. Ensuring the quality of the management methods used for the CSI process

4.6.2. Roles and Responsibilities

Table 22: Roles and Responsibilities Table for Continual Service Improvement

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop policies, guidance, and establish responsibilities for CSI	C	RA	C	C	C	C	C	C
Perform process monitoring/reporting	P	A	R	P	P	P	P	P
Ensure customer satisfaction while maintaining cost effectiveness	R	A	P	P	P	P	P	
Ensure quality of the management methods used for the CSI process		A	R					
Develop/refine vision, goals and objectives	C	RA	P	C	C			
Conduct baseline assessments	P	A	R	P	P	P	P	
Refine models		A	R					
Monitor/adjust measureable targets	P	A	R	P	P			
Define what you should/can measure	C	A	R		C			
Gather and analyze process data	P	A	R	P	P	P	P	P
Implement corrective action	P	A	R	P	P	P	P	P

5. IT SERVICES AND CAPABILITIES

IT Services Management and its associated processes were covered in detail in Section 4. This section focuses on those IT services and capabilities directly required by the Marine Corps for mission accomplishment. These services and capabilities can be broken down into three main categories:

- Security/Network Assurance
- Enterprise
- Regional/Local

Each of the ITSM processes discussed in Section 4 fully supports each of these services and capabilities.

5.1. SECURITY/NETWORK ASSURANCE

The MCNOSC is the designated Computer Network Defense Service Provider (CND-SP) for the Marine Corps. The CND-SP designation requires the following tasks be performed by MCNOSC:

- Perform CND Security Incident Management (SIM)
- Maintain the IA Security Infrastructure
- Perform Vulnerability Management
- Provide oversight and management of the Host Based Security System (HBSS)[1]
- Perform Security Scanning
- Conduct CND External Assessments
- Perform Incident Response
- Maintain INFOCON
- Manage C&A
- Manage PKI

5.1.1. Computer Network Defense Security Incident Management (SIM)

The CND Security Incident Management (SIM) system is a critical portion of the larger Common Operation Picture. The SIM aggregates and correlates CND related events from disparate systems into a consolidated view of all CND related events. The CND SIM can feed relevant alerts to the NetCOP or vice versa. This SIM supports customized views which will be created for each RNOSC.

[1] Includes Anti-Virus, Anti-Spyware

5.1.1.1. Objectives

A comprehensive CND SIM enables the MCNOSC to view individual events/alerts in an enterprise context. For example, a single event at a one location is potentially less significant than the same event occurring simultaneously at multiple locations.

5.1.1.2. Roles and Responsibilities

The MCNOSC maintains the configuration of the SIM and provides the required views to RNOSCs and MITSCs. Requests for specific SIM alerts or views must be coordinated with MCNOSC.

5.1.2. Information Assurance Security Infrastructure

The IA security infrastructure consists of those assets which provide enterprise security services. This includes the systems and connectivity required to manage network defenses, monitor network traffic and conduct enterprise vulnerability scanning/patching.

5.1.2.1. Objectives

A centrally managed IA infrastructure supports the ability to rapidly detect and respond to malicious activity. Additionally, it supports the continuity of IA services from the Alt NOSC when required.

5.1.2.2. Roles and Responsibilities

The MCNOSC is responsible for maintaining the IA security infrastructure. MITSC and local support may be required to support troubleshooting of infrastructure issues.

5.1.3. Vulnerability Management

5.1.3.1. Vulnerability Scanning

Vulnerability scanning in an enterprise capability maintained by the MCNOSC. MITSCs will leverage this capability to conduct the required scanning specified by USCYBERCOM, and additional scanning as required. Additionally, MCNOSC will be able to conduct scans with prior coordination with the MITSCs (with SA to RNOSCs) to minimize any unintentional network impact.

The vulnerability scanning capability will provide role-based views which can be tailored to specific AORs.

5.1.3.2. Vulnerability Patching

Vulnerability patching is an enterprise capability maintained by the MCNOSC. Due to the potential bandwidth implications of deploying software patches, MITSCs will be responsible for scheduling patch timing to avoid adverse impacts on the network. When required by an elevated threat to the network (e.g., active exploitation of the vulnerability), the MCNOSC will have the ability to push patches.

5.1.3.3. Objectives

The objectives of the Vulnerability Management Program is to provide comprehensive detection and mitigation of known vulnerabilities. The program will provide an enterprise view of vulnerable systems while simultaneously providing views tailored to RNOSC/MITSC.

5.1.3.4. Roles and Responsibilities

Table 23: Roles and Responsibilities Table for Vulnerability Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Enforce network level IA policies	RA			P	P	P	P	P
Perform System Security Analysis and Testing	R		A	I	P	P	C	C
IAVA patching	RA			I	P			
Employ Social Engineering Countermeasures	RA			I	CP	P		C
Define Intrusion Prevention Systems	RA			I	CP			
Define Software Update Services	R		A					
Audit collection and analysis	RA				CP		C	
Vulnerability lists/advisories	RA							
System Verification (standards/checklists)	RA	I		I	CP			
Vulnerability Assessment	RA			I	CP			
Threat Source Identification	RA							
Business Impact Analysis (BIA)	R	I	A	I	CP	P	C	C
Asset Criticality Assessment	R		A	I	CP		C	
Enterprise patch management/Manage enterprise patch server	RA							
Regional patch management/Manage regional patch servers	RA			I	CP			
Report CCIR events to MCNOSC MARCERT/Watch Officers	RA			P	CP	P	C	C

5.1.4. Host Based Security System (HBSS)

The HBSS is a centrally managed endpoint protection capability. Currently, HBSS includes a management agent, host intrusion prevention, policy auditor, anti-virus, anti-spyware, asset information and USB device control. The HBSS management server provides customizable dashboards that can provide situational awareness of HBSS managed systems.

MCNOSC will establish and maintain a baseline enterprise HBSS policy configuration based on USCYBERCOM requirements. HBSS events will be consolidated into the CND SIM for event correlation.

MCNOSC will create RNOSC and MITSC accounts which will provide regional visibility into HBSS events and individual component configurations. Additionally, with appropriate permissions, these accounts can manage individual HBSS components and create regional polices more restrictive than the enterprise policy.

5.1.4.1. Objectives

HBSS extends Defense-in-Depth to the network endpoints and protects individual workstations and servers from network compromise. Centralized management of HBSS allows for the enforcement of SIPRNet policies and supports the rapid deployment of additional policies required to protect against emerging network threats.

5.1.4.2. Roles and Responsibilities

Table 24: Roles and Responsibilities Table for HBSS

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Manage HBSS server	RA							
Manage HBSS signature repository	RA							
Define HBSS policies requirements for Programs of Record			RA					
Review HBSS dashboards for actionable alerts	RA			P	P	P	C	
Configure Regional HBSS Policies				A	R	P		

5.1.5. Security Scanning

As required, MCNOSC will develop and execute a capability to scan the SIPRNet for specific activity. This specialized scanning capability will be directed exclusively by MCNOSC.

5.1.5.1. Objectives

Security scanning allows the MCNOSC to rapidly identify systems of interest related to SIPRNet security events.

5.1.5.2. Roles and Responsibilities

Table 25: Roles and Responsibilities Table for Security Scanning

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Conduct enterprise network scanning on the SIPRNet	RA							
Conduct network scanning	RA				P			

5.1.6. CND External Assessments

The Marine Corps Information Assurance Red Team (MCIART) is a MCNOSC asset. The focus of the MCIART is to identify gaps or deficiencies in SIPRNet network defenses, policy, and/or user training. The MCIART will primarily focus on providing cooperative assessments as requested. Cooperative assessments benefit local personnel who establish the assessment scope, participate in the assessment and applicable remediation. No notice assessments are scheduled by the Commanding Officer MCNOSC to provide snapshot of the SIPRNet defensive posture.

HQMC/C4IA manages distributed IA Assessment Teams (Blue Teams). These teams support the internal, scheduled staff-assist system security assessments of Marine Corps systems world-wide. The Blue Team also support the internal system security self-assessments completed by the local IA staff on systems to which they have oversight and responsibility.

Actionable results or negative trends from these assessments will be promulgated to the entire NetOps community and to USCYBERCOM and other service CERTS.

5.1.6.1. Objectives

External CND assessments are used to identify security deficiencies and evaluate the effectiveness of security measures. The results are used to strengthen the security posture of the SIPRNet by recommending risk reduction countermeasures. Follow-on assessments will validate the effectiveness of these countermeasures.

5.1.6.2. Roles and Responsibilities

Table 26: Roles and Responsibilities Table for External CND Assessments

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Coordinate Red Team Assessments	R	A						
Coordinate Blue Team Assessments		RA			P			
Request Blue/Red Team Assessments				RA	P	C	C	C

5.1.7. Incident Response

MCNOSC provides perimeter boundary protection at each MITSC connection (B1)[1] and between each MITSC and supported sites (B2)[2]. The boundary protection includes a suite of routers, firewalls, and intrusion prevention systems. MCNOSC provides 24x7 monitoring of network sensors and ensures that all assessed incidents are reported to USCYBERCOM and/or coordinates with other Service CERTS as necessary.

MCNOSC formulates CND Response Actions (CND-RA) based on network activity, input from USCYBERCOM, other Service CERTS, NSA, or other indications and warnings.

CND-RAs will be promulgated in accordance with the NetOps C2 structure. When required, MCNOSC will coordinate in the most expeditious manner to the organization that can most quickly accomplish the desired effect. CND-RAs will generally be provided to all RNOSCs for situational awareness.

MCNOSC will conduct CND-RAs on enterprise assets for which it has administrative rights. MCNOSC personnel will conduct root-cause analysis of CND related events and network intrusions. Additionally, MCNOSC personnel will conduct enterprise forensic analysis of computer hardware.

RNOSCs and MITSC will conduct CND-RAs on all assets for which they have administrative rights. This includes the INFOCON requirements associated with returning an asset to a known secure baseline.

[1] B1 refers to the logical PoP/IA security suite 'configuration' or firewall rule set allowing internal (from within MCEN) and external (from outside MCEN/Internet) connectivity to the MCEN enterprise or MITSC-supported region's internal systems and addresses. Refer to section 5.2.1.1 for further information on the PoP/IA Security Suite.

[2] B2 refers to the logical PoP/IA security suite 'configuration' or firewall rule set allowing connectivity to internal systems (from within MCEN through the regional B1) and external systems (from outside MCEN/Internet) to B/S DMZs. B2s can be re-configured to operate like a B1 in contingency operations if the regional B1 fails. Refer to section 5.2.1.1 for further information on the PoP/IA security suite.

5.1.7.1. Objectives

An effective incident response process allows for the rapid detection and mitigation of malicious activity. CND-RA direct the actions required to prevent similar activity and benefit all systems proactively.

5.1.7.2. Roles and Responsibilities

Table 27: Roles and Responsibilities Table for Incident Response and Analysis

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Monitor for unauthorized/malicious activity	RA			I	P	P	C	C
Report potential security incidents	RA			I	P	P	C	C
Direct CND-RA	RA							
Execute appropriate CND-RA	RA			P	P	P	C	C
Collect and preserve evidence	RA			I	P	P	C	C
Analyze and detect malicious code and incidents	RA							
Conduct forensic analysis	RA							
Contain incidents and eradicate vulnerabilities	RA			I	P			
Recover to pre-incident state	RA				P	P	C	C
Respond to Law Enforcement requests	R	A		P	P	P		

5.1.8. INFOCON

The Deputy Commandant for Plans, Policies, and Operations (PP&O), in coordination with the HQMC Director C4, is authorized to set the service wide INFOCON level. While INFOCON levels can be established regionally, in most cases the MCEN will maintain a single enterprise INFOCON level based on the highest regional level.

The MCNOSC, through NetOps reporting chains, will provide service response to USCYBERCOM on all INFOCON matters to include operational impact assessments. These impact assessments will be conducted in anticipation of changing INFOCON level or prior to implementing a Tailored Response Option (TRO).

RNOSCs and MITSCs will coordinate with the regional COCOM on potential changes to INFOCON levels in their specific AOR. This coordination must be conducted with MCNOSC participation to ensure inter-MITSC enterprise functionality is not adversely impacted. Regional Commanders are required to develop and publish specific INFOCON procedures for their AOR to include garrison and deployed environment.

5.1.8.1. Objectives

The INFOCON system provides a framework within which commanders can increase the measurable readiness of their networks to match operational priorities. Key to this strategy is a shift from a threat focus to a readiness focus. The system provides a framework of prescribed actions and cycles necessary for reestablishing the confidence level and security of information systems for the commander.

5.1.8.2. Roles and Responsibilities

Table 28: Roles and Responsibilities Table for INFOCON Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Establish Service INFOCON Level		RA						
Establish Regional INFOCON Level				RA				
Coordinate with COCOMs in support of regional INFOCON changes.	A			R				
Provide input to INFOCON Operational Impact Assessments	RA		P	C	CP	P	C	C
Provide Operational Impact Assessments to USCYBERCOM	RA							
Perform all INFOCON tasks on enterprise assets.	RA							
Perform all INFOCON tasks on regional assets.				A	R			
Perform all INFOCON tasks on local assets.					A	R		
Implement INFOCON TROs	RA			C	CP	P	C	
Develop TTPs required to support any INFOCON tools or TROs.	RA				CP			
Conduct a quarterly review of published TROs and prepare implementation guidance.	RA			C	CP	P		
Monitor changes to INFOCON	R	A		P	P			
Perform actions to comply with INFOCON requirements.	RA			I	CP	P	C	
Monitor and validate all system baseline changes	RA			I	CP	P	C	
Return systems to a know secure configuration as required	RA			I	CP	P	C	

5.1.9. Public Key Infrastructure (PKI)

The need to provide more robust and secure authentication methods on the DoD SIPRNet led to a consensus that implementing hardware based PKI token can provide the higher security posture desired on the SIPRNet. Current user name/password authentication methods create security gaps for users; difficult password generation schemes only hamper the end user's ability to effectively use the network. The ability to take one's credentials from location to location without securing it is especially advantageous to the warfighter during highly mobile missions and those requiring split-jump operations where securing a token would be impractical and an undue burden on the warfighter's ability to rapidly respond to the mission. Another benefit of a portable token is that the warfighter's credentials are always available for use. In FY09, DoD PKI Program Management Office will conduct a pilot and push for an Initial Operational Capability (IOC)/FOC for a new SIPRNet hardware token in a smartcard form factor beginning in FY10. The implementation of a hardware token on SIPRNet will precipitate a new token infrastructure across the SIPRNet for token issuance, a certificate validation infrastructure, additional client hardware and software and implementation of the use of DoD PKI for access to the SIPRNet, SIPRNet Resources, and digital signing and encryption of email.

5.1.9.1. Concept of Operations

The MCNOSC PKI Section will implement the current and expanded DoD PKI on the SIPRNet. Management and configuration of DoD products, certificate issuance, and certificate validation services registration authority operations will be centralized at the MCNOSC and implemented in a distributed fashion across the SIPRNet.

5.1.9.2. Roles and Responsibilities

Table 29: Roles and Responsibilities Table for PKI

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Enterprise								
Registration Authority (RA)	RA							
Register; manage; and control the subordinate Local Registration Authorities (LRA) with DISA	RA							
Assure the binding of public keys with respective user identities.	RA							
Approve/renew/terminate LRAs privileges	RA							
Update Certificate Revocation Lists (CRLs)	RA							
Revoke certificates by any RA	RA							
Add/modify/delete directory entries	RA							
Provide training and certification for LRAs	RA							

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
LRA	RA							
Authenticate/register individual subscribers within their local area of responsibility	RA				P	C		
Request a certificate be revoked (based on owner request or LRA Information Systems Security Officer (ISSO)	RA				P	C		
Resolution of escalated issues associated with Tier I or Tier II Support	RA							
RA services: PKI certificate issuance and revocation of software certificates	RA							
PKI Engineering support: Maintenance of configuration, installation, training documentation, and implementation guidance	RA							
Regional								
Maintenance and troubleshooting of PKI services:	RA				P			
PKI hardware tokens, software certificates, server certificates, and validation services	RA							
Installation and configuration of smartcard reader, middleware, certificate validation software, and DoD Certificate Authority (CA) Root Store					A	R		
PK-enablement of servers and configurations					A	R	C	
PKI roots and USMC CA distribution of domain controller certificates	RA							
Repeater hardware	RA							
Software maintenance	RA							
Local								
Installation, configuration, maintenance, and troubleshooting to support PKI hardware tokens, software certificates, server certificates and validation services						A		
Installation and configuration of smartcard reader, middleware, certificate validation software, and DoD CA Root Store						A		
Troubleshooting for errors in PKI services					A	R		
PK-enablement of servers and configurations that supports only DoD						A	C	
PKI roots and USMC CA distribution of domain controller certificates					A	R	C	

5.2. ENTERPRISE

MCEN SIPRNet enterprise services are provided by the MCNOSC through its staff in MCB Quantico and MCNOSC Detachment staff co-located with the RNOSCs/MITSCs and EITCs. Enterprise services are generally defined as the common physical/virtual infrastructure, applications, and services operated and managed in support of all users and organizations across the Marine Corps. This enterprise implementation is meant to provide a dependable, robust, and secure communication backbone that provides high availability/disaster recovery and supports all Marine Corps missions.

5.2.1. WAN Services

5.2.1.1. WAN and PoP Security Infrastructure

Referring to Figure 19, the WAN and PoP Security Infrastructure includes:

- All equipment (hardware and software) from the Boundary 1 (B1) Point of Presence (PoP), through the Asynchronous Transfer Mode (ATM) SIPRNet backbone, to the Defense Information Switch Network (DISN) Black Core (except those operated by DISA.) The PoP/IA Security Suite consists of a screening router, outer switch, firewall configured with a B1 policy, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), audit server, Demilitarized Zone (DMZ)/inner switch, audit server, PoP router, High Assurance Internet Protocol Encryptor (HAIPE) gateway, Domain Name System (DNS) and audit servers.
- All equipment (hardware and software) within the Boundary 2 (B2) PoP/IA Security Suites

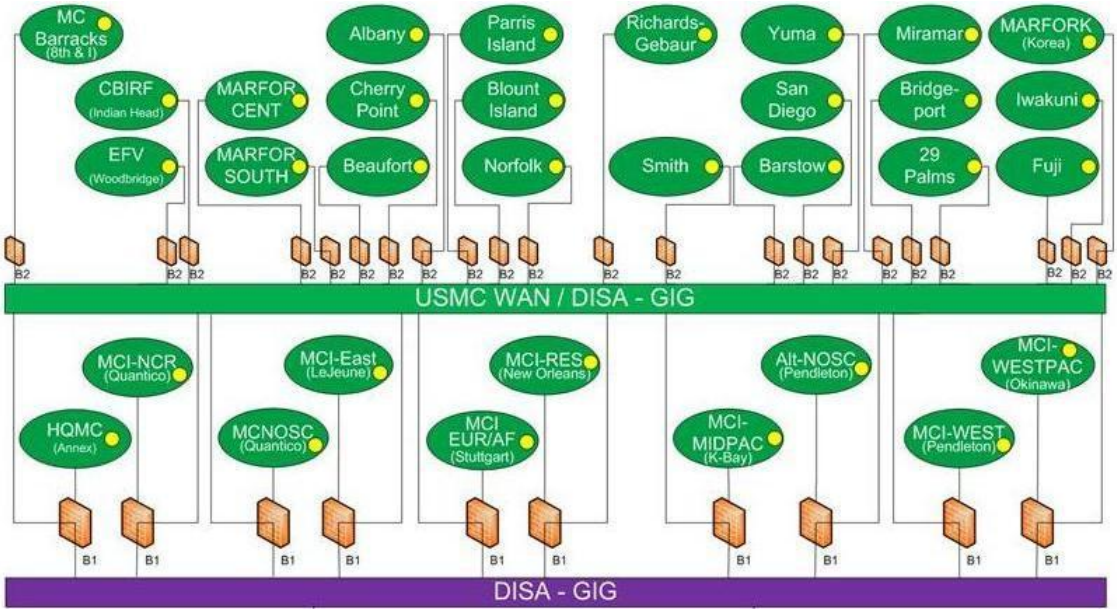

Figure 19: SIPRNet Enterprise

5.2.1.1.1. Roles and Responsibilities

Table 30: Roles and Responsibilities Table for WAN and PoP Security Infrastructure

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Provide technical oversight and implementation of USMC networks	RA							
Establish IP requirements for USMC	RA							
IP allocation/tracking for USMC subnets	RA							
Establish all naming standards for USMC IT assets	RA							
Define Requirements (Routing, Management, Remote Access, Protocols, and Standards)	RA							
Validate Requirements (Routing, Management, Remote Access, Protocols, and Standards)	RA							
Establish Quality of Service (QoS) Methods	RA							
Define Virtualization Services	RA							
Define Egress Services	RA							
Install/configure/remove WAN hardware/software assets per section above IAW enterprise change management processes	RA							
Perform Requirements Analysis	RA							
Develop Cost Analysis	RA							
Provide and Maintain Enterprise Security Services	RA							
Maintain the USMC Firewall Policies (B1/B2)	RA							
Manage B1/B2 PoP suite IAW entreprise change management processes.	RA							
Conduct 24x7 support operations and troubleshooting of WAN infrastructure	RA							
Review proposed request for new and existing applications, ensuring that all requests fall within the Firewall Policy and that all associated documentation is in order.	RA							
Coordinate with the Base G6 representatives to discuss future base architecture and SIPRNet access	RA			I	P			
Provide technical support in the area of routers, firewalls, DNS and circuits	RA							
Review system check in order to detect security alert patterns	RA							
On-site integration of emerging firewall technologies	RA							
Resolve and track all customer related connectivity issues through the PoP Architecture	RA							
Document procedures, standards and policies related to the information architecture	RA							
Provide for the accountability and physical security of SIPRNet PoP equipment.	RA							
Notify the operational forces in advance of any planned or scheduled event or activity that may affect	RA							

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
the operation. For unplanned emergency situations, notification will be made as soon as practical. Notification must be made to the MCNOSC Watch Officer via telephone or by electronic mail.								
Notify the MCNOSC in advance of any planned or scheduled event or activity that may affect the operation of B1/B2 PoP equipment, such as a scheduled power outage or a physical relocation of equipment. For unplanned emergency situations, notification will be made as soon as practical. Notification must be made to the MCNOSC Watch Officer via telephone or by electronic mail.				A	R	P		C
Notify the MCNOSC Watch Officer ASAP whenever equipment failure or service degradations are detected.				A	R	P	C	C

5.2.1.2. Circuits

Figure 20 below depicts the current circuit provisioning process. Circuit services are described as any and all inter-site connections which enter or leave the confines of a Marine Corps B/S, installation, headquarters, or federal building regardless of mileage distance. It includes all long-haul telecommunication services including voice, data, video switching, transmission services and associate network management, to include regional service, Metropolitan Area Networks (MANs), and ATM edge devices.

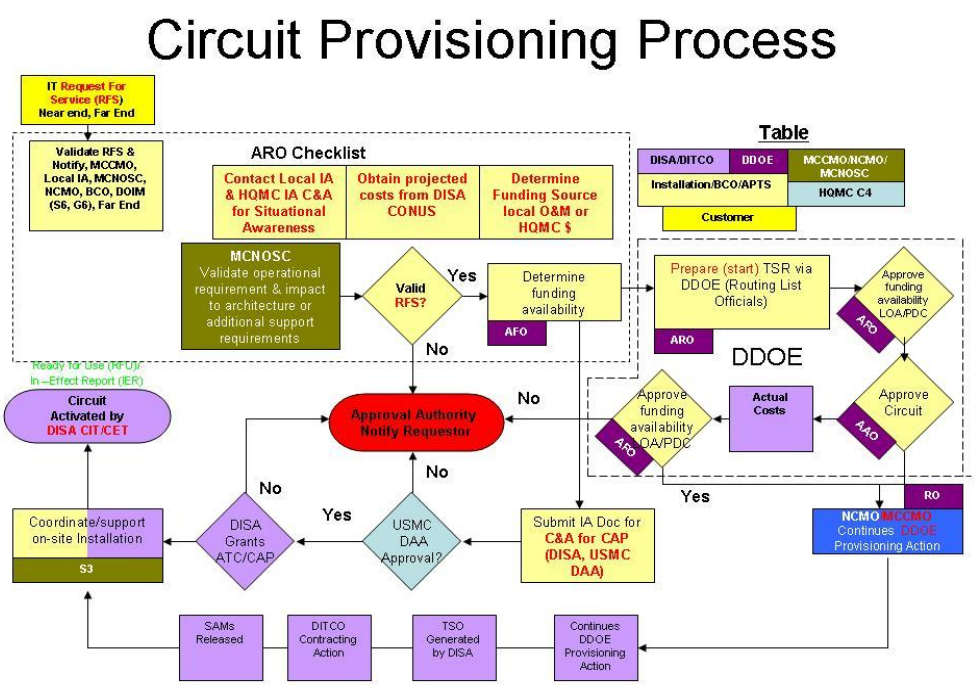

Figure 20: Circuit Provisioning Process

5.2.1.2.1. Roles and Responsibilities

Table 31: Roles and Responsibilities Table for WAN Circuits

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Circuit Request to HQMC C4/CP	RA			P	P	P		
Validation and Impact/Bandwidth Assessment	RA							
Requester submits Telecommunication Service Request (TSR) via DDOE	RA			P	P	P		
Circuit Approval (CP)		RA						
Forwards TSR as valid rqmt to NCMO (CP)		RA						
Determine/Obtain Funding (CR)		RA						
AFO forwards funding to NCMO (CR)		RA						
Coordinate/support on-site engineering	RA							
Requester submits SAA to HQMC IA C&A	RA			P	P	P		
Grants ATC (DISA)								RA
Circuit Installation – Telco (Telco)								RA
Circuit Installation - Customer Premise (DISA)	P							RA
Assign PDC(NCMO)								RA
Circuit Provisioning (Naval Circuit Management Office (NCMO))								RA

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Circuit Activation (DISA)								RA
End to End Testing (DISA)								RA
Circuit Acceptance	RA			P	P	P		
Retire Circuits	RA			P	P	P		

5.2.2. Enterprise Directory Messaging (EDM) and Storage

Enterprise Directory Messaging (EDM) and Storage provides SIPRNet e-mail and official messaging directory services maintenance and synchronization.

5.2.2.1. Roles and Responsibilities

Table 32: Roles and Responsibilities Table for Enterprise Directory, Messaging and Storage

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Provide policy for patching/updating of WAN equipment	RA							
Domain Administration (health and management of the Domain/replication)								
Establish all USMC naming standards for directory service entries	RA				C	C		C
Administer the single AD Forest (Root Domain)	RA							
Domain Administration (health and management of the Domain/replication)	RA				I	I		I
Managing domain replication for MCW, and DMS, (including domain controller installation/configuration/removal)	RA				I	I		I
Administering Domain controllers for MCW domain	RA				I	I		I
Administering Domain controllers for DMS	RA				I	I		I
Administer tactical domains (1MEF, 2MEF, 3MEF, and 4MEF)	I			I	C	P		RA
Control domain-level Group Policy Objects (GPO)	RA				I	I		I
Organizational Unit (OU) Administration								

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Establish OU naming standards	RA				I	I		I
Manage and apply top level permissions hierarchy	RA				C	I		I
Administer (creation/modification/removal) the top level regional OU down to the B1/B2 OU	RA				I	I		I
Manage/maintain any and all OU hierarchy and structure below the MITSC OUs level					RA	P		P
Manage objects at MITSC OU level (computers, users, groups)					RA	P		P
Manage and apply B1/B2 permissions hierarchy					RA			
Manage B/S objects at OU level (computers, users, groups)					RA			
Define, apply, and link GPO at the Enterprise OU level	RA				I	I		I
Define, apply, and link GPO at the MITSC OU level					RA	CP		P
Define, apply, and link GPO at the B/S/OPFOR level					RA	CP		CP
DNS								
Managing MCW DNS server	RA				I	I		I
Manage Command DNS servers					RA			
Manage MCW DNS zone	RA							
Manage Command zones					RA			
Switches (Public, VMKernel, Private)	RA							
Upgrade IOS	RA							
Manage/maintain configuration	RA							
Configuration Backups	RA							
Hardware maintenance/replacement	RA							
Storage Area Network (SAN)								
Upgrading/patching operating system	RA							
Hardware maintenance/replacement	RA							
Disk configurations (aggregates volumes/logical unit numbers)	RA							
Configuration management IAW Enterprise configuration management process	RA							
Maintain replication path to designated COOP site	RA							
Manage SAN Common Internet File System (CIFS) shares	RA							
Virtual Infrastructure								
Upgrading/patching operating system (physical ESX and VirtualCenter)	RA							

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Hardware maintenance/replacement (physical ESX)	RA							
Configuration management IAW enterprise configuration management process (physical ESX)	RA							
Manage High Availability (HA) functions	RA							
DMS								
Provides programmatic oversight for the implementation of DMS Proxy Solution and coordinates policy and program Support.		RA						
Provides DMS reporting to external organizations to include DON and DoD.		RA						
Directs Marine Corps representation with external organizations on DMS related issues.		RA						
Ensures training is available for ACC/Tactical DMS (ACC/TDMS) operators and CAW personnel.		RA						
Ensures sufficient DMS trained manpower for operation of garrison and tactical ACC/TDMS.		RA						
Coordinates development of Joint DMS and CAW policy to support USMC operations.		RA						
Participates in DISA DMS working groups.		RA						
Provides Marine Corps DMS and CAW policy as required.		RA						
Provides Marine Corps DMS and CAW policy IA posture that maintains compliance with Marine Corps C&A practices throughout fielding and life-cycle management of DMS-related products.		RA						
Provides DMS and IA program management responsibilities among DoD DMS program participants that include acquisition and deployment of DMS components and IA solutions products (CAWS and Fortezza cards/tokens).			RA					
Provide DMS and CAW/Fortezza PKI Program Manager functions.			RA					
Assist in Proxy implementation/coordination efforts among various DMS program participants for their ACC/TDMS and base infrastructure support, including but not limited to external organizations such as DISA, Army, Air Force, and Navy DMS program management offices.			RA					

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Plan, program, and implement DMS within the Marine Corps. Develop/update architectures and related concept of operations for the implementation of new products.			RA					
Provide hardware, software, and licensing to support the Marine Corps ACC/TDMS, and the DMSCOC, as required.			RA					
Provide funding for new equipment training for ACC/TDMS operators.			RA					
Provide ACCS on site technical and operational support for the 1st year (if required) of new DMS products upon implementation.			RA					
Provide life cycle management of hardware and software support for the Marine Corps ACCS/TDMS, DMS schoolhouse and DMSCOC.			RA					
Develop and manage DMS related contracts as required.	C		RA					
Report DMS acquisition status to HQMC C4 quarterly.			RA					
Participate in DMS implementation working groups.			RA					
Perform role as the Marine Corps CAW approval authority.			RA					
Develop and ensure compliance of Marine Corps CAW and certification practice statement and distribution and management of DMS-related IA products.	C		RA					
Provide technical assistance and ensure life cycle support in the fielding and implementation of CAWS and the preparation of NSA certification authority (CA) request and update forms.			RA					
Maintain the DMS IT C&A (DITSCAP) package for USMC DMS messaging.			RA					
Operate the Marine Corps DMS Central Operations Center (DMSCOC).	RA							
Direct, control and manage DMS operations within the Marine Corps.	RA							
Provide Direct interface with the DISA-managed regional Network Operations Center (NOC).	RA							
Develop and publish Marine Corps procedures for DMS operations.	RA				C			
Provide USMC DMS technical guidance	RA							

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
and USMC DMS operational standards.								
Conduct annual site visits/audits for all ACCS.	RA							
Act as the Marine Corps DMS RA for X.500 registration.	RA							
Manage DMS directory operations.	RA							
Provide Marine Corps address list management.	RA							
Act as the DMS configuration manager.	RA							
Provide 24 hour DMS Help Desk support for garrison and tactical sites.	RA							
Report DMS progress to HQMC C4 monthly.	RA							
Provide PKI services adequate to support DMS domain Fortezza.	RA							
Participate in DMS operational working groups.	RA							
Manage DMS X.500 Directory	RA							
Provide Marine Corps Mail List Management	RA							
Ensure all DMS operators and organizational releasers, drafters, and readers within their particular command, organization or AOR comply with the policies and procedures contained in appropriate Naval Telecommunications Procedure (NTP) documents, DISA circulars, USMC Site Operation Guidelines (SSOG), MCNOSC SOPs and this publication.						RA		
For all SIPRNet Marine Corps DMS systems, the ACCS and TDMS personnel will operate, manage and monitor their portion of the DMS infrastructure components.						RA		
ACC directly interfaces with the MCNOSC/DMSCOC to resolve communication difficulties within their region.						RA		
Provide DMS messaging services to USMC organizations and releasers within the theater of operation the ACC/TDMS supports.						RA		
Coordinate disaster recovery operations with alternate sites supporting ACC.						RA		
Support disaster recovery servers hosted within the ACC.						RA		

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Oversee the appointment of OMPOC and alternate from each supported organization.						RA		
Provide training to the organizational messaging point of contact (OMPOC) designated by the supported commands.						RA		
Coordinate with the supported organizations, maintaining an agreement to create and sign the X.509 on behalf of the commands the ACC supports on the enterprise AMHS/CP-EXP.						RA		
Maintain online copies of incoming and outgoing messages for a minimum 30 days plus the current day for compliance with trace and retransmission requirements.						RA		
Retain online copies of incoming and outgoing messages for a minimum of 30 days and archived messages for a minimum of one year or more based on Command requirements.						RA		
Provide user training for Commands within their AOR.						RA		
Submit reports to MCSC and the DMSCOC as required.						RA		
Immediately report lost or compromised Fortezza cards to the Information System Security Officer (ISSO).						RA		
Comply with Marine Corps Certificate Policy Statement (CPS) for Fortezza/CAW PKI.						RA		
Ensure a primary and backup CAW operator and CAW SA/ISSO are appointed and have completed required training.						RA		
Ensure DMS organizations are registered and their releaser certificates are properly posted in the X.500 Directory.						RA		
Ensure that CRL are posted in accordance with current regulations.						RA		

5.2.3. Real-Time Services

Real-Time Services is an umbrella that covers those elastic services in which the delivery of the data packets is critical. It typically includes such services as video teleconference (VTC) and VoSIP.

VTC allows users to communicate using audio and video (H.323) over an IP network. VoSIP provides voice communications via the SIPRNet, allowing users in any branch of the DoD to talk with one another. While Table 33 below identifies MCNOSC as responsible/accountable for SIPRNet VTC services, this is predominantly for technical guidance associated with installation, configuration, operation, and scheduling. Until an enterprise-wide VTC system is in place, individual sites will continue to procure, install, schedule, and manage SIPRNet VTC facilities through their MITSC or delegated B/S G/S-6.

5.2.3.1.1. Roles and Responsibilities

Table 33: Roles and Responsibilities Table for Real-Time Services

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
VTC (Video Teleconference)								
Install/configure/remove equipment IAW enterprise change management processes	RA		I		CP	P		P
Scheduling	RA		I		CP	P		P
Engineer/design enterprise VTC services	RA							
Maintain/operate VTC facilities	P	P	P	P	RA	P	P	P
VoSIP[1]								
Design, implement, and integrate VoSIP	RA							
Assess current voice needs	RA				P			
Assess integration needs for Voice	RA							
SIP signaling	RA							
H.323 signaling	RA							
Media Gateway Control Protocol (MGCP)	RA							
Network Address Translation (NAT) issues	RA							
Analog terminal adapter (ATA)	RA							
Firewall support	RA							
Session border controllers	RA							
Trunking requirements	RA							
Establish Availability	RA							
Establish Quality of Service (QoS)	RA							

[1] Note: At the time of drafting the SIPRNet COE, VOSIP is in the planning phase. Once complete, the Roles and Responsibilities will be updated.

5.2.4. Data Backup

This includes backup support for data at the enterprise level; specifically enterprise-wide applications and configurations operated and managed in support of all users and organizations across the Marine Corps. See section 5.3.7. for all other non-enterprise applications.

5.2.4.1. Roles and Responsibilities

Table 34: Roles and Responsibilities Table for Enterprise Data Backup

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Perform enterprise application data/database backups	RA							
Manage enterprise file share replication	RA				I			
Restore enterprise application data/database backups	RA							

5.2.5. Application/Data[1]

This generally includes enterprise provisioned, hosted, or managed software applications in particular collaboration tools, portals, and databases. Additionally, it encompasses data and connectivity support.

5.2.5.1. Roles and Responsibilities

Table 35: Roles and Responsibilities Table for Enterprise Application/Data

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Identify enterprise application/data requirements	RA	C	C	C	C			
Validate enterprise application/data		C	RA					

[1] Note: The MCEITS is a future capability that will provide this service/capability at the Enterprise level. Controlled and managed by MCNOSC, MCEITS will provide enterprise capabilities through MCEITS Platforms, an ESDE and the EAE. The ESDE is the Marine Corps' environment for data management and enterprise services that support warfighting and business mission areas. The EAE provides users access to MCEITS provided and hosted enterprise-class systems and applications.

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
requirements								
Software procurement /license management			RA					
Establish/maintain enterprise application/data transport	RA							
Establish/maintain enterprise application/data security	RA							
Establish/maintain enterprise application/data identity management	RA							
Install server applications IAW enterprise change management process	RA				P			
Install client applications IAW enterprise change management process					RA			
Provide enterprise application/data backup support	RA				CP			
Provide software and connectivity support (hands on/on call), as assigned by or coordinated through the ESD					RA			
Training (hands on/distance learning)					RA			
Application/data access	RA	P	P	P	P	P	P	P

5.3. REGIONAL/LOCAL

In the USMC regionalized support concept, regional services are provided by the MITSCs through the MITSC staff with oversight and direction by the RNOSCs. Local services are provided by the MITSCs through the B/S G6s and their touch labor. Enterprise-managed ITSM processes (i.e., Incident and Problem Management), applications, and an ESD support this regionalization concept through efficient employment of standardized tools and processes, while keeping responsive technical and mission-focused expertise nearer to the customer. Refer to section 4 for more information on ITSM processes, section 4.5.1 for the ESD, and section 5.2 for more information on Enterprise services. Note: This is subject to update as the detailed E-ITSM processes are further developed or refined.

5.3.1. BAN/LAN Infrastructure

This generally includes physical/virtual infrastructure providing connectivity from the enterprise to the end user desktop/laptop. This typically includes the inside/outside cable plant and routing/switching infrastructure.

5.3.1.1. Roles and Responsibilities

Table 36: Roles and Responsibilities Table for BAN/LAN Infrastructure

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Identify regional BAN/LAN infrastructure requirements	C	A	I	I	R	P		P
Validate regional BAN/LAN infrastructure requirements	C	A	I	R	P	P		P
Maintain list of MAC levels of all regional SIPRNet information systems/network devices				RA				
Conduct mission criticality assessments				A	R			C
Conduct Operational Impact Assessments to regional incidents				A	R			C
Conduct Risk Assessments				A	R			I
Plan, engineer, design, and install BAN/LAN infrastructure	C		RA			C		
Maintain/provide up-to-date network configuration data	C		RA		CP	CP		C
Maintain/provide up-to-date equipment accountability					RA	C		C
Manage the regional IT infrastructure					RA			
Install cable trunks and fiber runs IAW enterprise change management processes					RA	P		C
Operate, and maintain regionally managed infrastructure and systems, including the hosting of tactical systems supporting the operating forces					RA			
Maintain high-availability production environment for MAGTF staff members.					RA			
Lifecycle Management	C		RA			P		
Install/configure/remove routers, switches, and other BAN/LAN devices IAW enterprise change management processes	C				RA	CP		C

5.3.2. End-User E-mail

E-mail service for end users includes all support for client-based and web-based electronic mail.

5.3.2.1. Roles and Responsibilities

Table 37: Roles and Responsibilities Table for End-User E-mail

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Identify regional e-mail requirements	C	A	I	I	R	P		P
Validate regional e-mail requirements	C	A	I	R	P	P		P
E-mail account creation, modification, and deletion				I	RA	CP		P
Add/remove GAL entries				I	RA	CP		P
Manage mailboxes (restrictions, attachment size, storage, etc.) per existing policy				I	RA	C		C
Manage public folders				I	RA	CP		P
Administer PKI signature/encryption					RA	CP		C
Provide GAL synchronization with directories and provide certificates in GAL	C				RA			
Installation/removal of e-mail client software					RA	CP		P
Other technical support (hands on/on call), as assigned by or coordinated through the ESD					RA	CP		P
Training (hands on/distance learning)					A	R		P

5.3.3. File Sharing

This generally includes the creation, modification; removal, permission management, and end user support for network file shares and drive mappings.

5.3.3.1. Roles and Responsibilities

Table 38: Roles and Responsibilities Table for End-User File Share

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Manage file servers (patching)					RA			
Identify regional file share requirements	C	A	I	I	R	P		P
Validate regional file share requirements	C	A	I	R	P	P		P

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Create/modify/remove file shares					RA	P		P
Manage Distributed File System (DFS)-based file share permissions					RA	P		P
Provide technical support (hands on/on call) as coordinated through the MITSC Service Desk					RA	P		
Training (hands on/distance learning)					RA	P		

5.3.4. Print/Scan/Fax

This generally includes the creation, modification, removal, permission management of end user devices, network services, and software driver support for end-user printing, scanning, and faxing.

5.3.4.1. Roles and Responsibilities

Table 39: Roles and Responsibilities Table for Print/Scan/Fax

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Identify regional printing/scanning/faxing requirements	C	A	I	I	R	P		P
Validate regional printing/scanning/faxing requirements	C	A	I	R	P	P		P
Maintain equipment accountability						RA		P
Manage print/scan/fax devices IAW enterprise change management processes					RA	CP		C
Procure and install associated disposables and supplies						RA		P
Provide technical support (hands on/on call) as coordinated through the Enterprise Service Desk					RA	P		
Training (hands on/distance learning)			A		R			

5.3.5. Secure Mobile Environment Portable Electronic Device (SMEPED)

This generally includes the issuance, accountability, and end-user support for Secure Mobile Environment Portable Electronic Devices (SMEPED), which provide wireless voice transmission up to Top Secret level and data communications up to Secret level.

5.3.5.1. Roles and Responsibilities

Table 40: Roles and Responsibilities Table for SMEPED

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Identify regional SMEPED requirements	C	A	I	I	R	P		P
Validate regional SMEPED requirements	C	A	I	R	P	P		P
Issue SMEPEDs					RA			
Maintain equipment accountability					RA	P		P
Provide technical support (hands on/on call) as coordinated through the ESD					RA			
Coordination with service provider					RA			
Training (hands on/distance learning)					RA			

5.3.6. Desktop/Laptop

This generally includes procurement, management, and accountability of end-user client workstations (desktops/laptops) and associated software/peripherals.

5.3.6.1. Roles and Responsibilities

Table 41: Roles and Responsibilities Table for Desktop/Laptop

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Participate in Marine Corps Enterprise Desktop Standardization (MCEDS) Integrated Product Team (IPT)	P	P	RA		C	C	C	C
Identify regional desktop/laptop hardware/software/peripheral requirements	C	A	I	I	R	P		P
Validate regional desktop/laptop hardware/software/peripheral requirements	C	A	I	R	P	P		P
Maintain hardware accountability						RA		P
Determine mission category for all desktops/laptops	I		I	I	RA	CP		P
Desktop/laptop procurement (MCHS)			RA		CP	CP		P
Software procurement /license management			RA		CP	CP		P
Develop deployment plan (Phased, Regional, etc.)			RA		CP	P		P
Stage new hardware with software build			A		R			
Deliver desktop/laptop to end-user			A		R	P		P

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Deliver IA control to desktop/laptop	R		A					
Software installation/removal	CP		A		R	P		P
Migrate user data (from old machine) to allocate storage (SAN, NAS, etc.)			A		R	CP		P
Provide technical support (hands on/on call) as coordinated through the ESD					RA	CP		C
Training (hands on/distance learning)					RA			

5.3.7. Data Backup

This generally includes support for backing up data created by the end-user's client applications and stored locally, on a network file share, or SAN.

5.3.7.1. Roles and Responsibilities

Table 42: Roles and Responsibilities Table for End-User Data Backup

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Perform regional/local application data/database backups					RA	I		I
Manage file share replication	CP				RA	I		I
Manage data back-ups on the SANs at the Regional MITSCs	CP				RA			
Backup/restoration of e-mail accounts					RA	C		C
Perform desktop/laptop backups					C	RA		P

5.3.8. Application Deployment and Data Management[1]

Prior to software deployment, this responsibility lies with FAMs. Application deployment and data management generally includes regionally- or locally- provisioned, hosted, or managed software applications – in particular collaboration tools, portals, and databases. Additionally, it encompasses data and connectivity support.

[1] Note: The MCEITS is a future capability that will provide this service/capability at the Enterprise level. Controlled and managed by MCNOSC, MCEITS will provide enterprise capabilities through MCEITS Platforms, an ESDE and the EAE. The ESDE is the Marine Corps' environment for data management and enterprise services that support warfighting and business mission areas. The EAE provides users access to MCEITS provided and hosted enterprise-class systems and applications.

5.3.8.1. Roles and Responsibilities

Table 43: Roles and Responsibilities Table for Application Deployment and Data Management

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Software procurement /license management			RA					
Establish/maintain regional application/data transport					RA			
Establish/maintain regional application/data security					RA			
Establish/maintain regional application/data identity management					RA			
Install server applications IAW enterprise change management process	RA				P			
Install client applications IAW enterprise change management process	CP				RA	P		P
Provide regional application/data backup support	CP				RA			
Provide software and connectivity support (hands on/on call) as coordinated through the ESD					RA			
Training (hands on/distance learning)					RA			
Application/data access	RA	P	P	P	P	P	P	P

APPENDIX A: ACRONYMS

ACRONYM	DEFINITION
AAO	Approved Acquisition Objective
ACC	Area Control Center
ACMC	Assistant Commandant of the Marine Corps
AD	Active Directory
ADCON	Administrative Control
AMHS	Automated Messaging Handling System
AOR	Area of Responsibility
AOR	Assumption of Responsibility
ASVAB	Armed Services Vocational Aptitude Battery
ASN (RD&A)	Assistant Secretary of the Navy Research Development and Acquisition
ATA	Analog Terminal Adapter
ATM	Asynchronous Transfer Mode
B/S	Base/Station
B1	Boundary One
B2	Boundary Two
BAN	Base Area Network
BIA	Business Impact Analysis
BuRAS	Broadband Unclassified Remote Access Service
C&A	Certification and Accreditation
C.O.	Commanding Officer
C2	Command and Control
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers and Intelligence
CA	Certificate Authority
CAB	Change Advisory Board
CAC	Common Access Cards
CAW	Certificate Authority Workstation
CC/S/As	Combatant Commanders/Services/Agencies
CCIR	Commanders Critical Information Requirements
CDD	Capability Development Document
CDR	Capabilities Development Roadmap
CDRT	Capabilities Development Roadmap Tracker
CDRUSSTRATCOM	Commander, USSTRATCOM
CfM	Configuration Management
CG	Commanding General
ChM	Change Management
CI	Configuration Items
CIFS	Common Internet File System
CIP	Critical Infrastructure Protection
CJCSI	Chairman Joint Chiefs of Staff Instruction

ACRONYM	DEFINITION
CJCSM	Chairman Joint Chiefs of Staff Manual
CMC	Commandant of the Marine Corps
Cmd	Command
CMDB	Configuration Management Database
CMS	Configuration Management System
CND	Computer Network Defense
CND-RA	Computer Network Defense Response Action
CND-SP	Computer Network Defense Service Provider
COA	Courses of Action
COCOM	Combatant Command
COE	Concept of Employment
COI	Community of Interest
COMMARFOR	Commander of Marine Forces
COMSEC	Communication Security
CONOPs	Concept of Operations
COOP	Continuity of Operations Plan
COP	Common Operational Picture
CPS – Policy	Certificate Policy Statement
CPS – Practice	Certificate Practice Statement
CRL	Certificate Revocation Lists
CSI	Continuous Service Improvement
CTO	Communication Tasking Orders
CVI	Certificate Validation Infrastructure
DAA	Designated Approval Authority
DB	Database
DC	Domain Controller
DFS	Distributed File System
DHS	Department of Homeland Security
DIACAP	Department of Defense (DoD) Information Assurance Certification & Accreditation Process
DISA	Defense Information System Agency
DISN	Defense Information Switch Network
DITSCAP	Department of Defense (DoD) Information Technology Security Certification & Accreditation Process
DML	Definitive Media Library
DMS	Defense Messaging System
DMSCOC	Defense Messaging System Central Operations Center
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DoDI	Department of Defense Instruction
DON	Department of Navy
DOTMLPF	Doctrine, Organization, Training Materiel, Leadership and Education, Personnel, and Facilities

ACRONYM	DEFINITION
DS	Direct Support
E-ITSM	Enterprise Information Technology Service Management
E-LMR	Enterprise Land Mobile Radio
EAE	Enterprise Application Environment
EDM	Enterprise Directory Messaging
EFDS	Marine Corps Expeditionary Force Deployment System
EITC	Enterprise Information Technology Center
EKMS	Electronic Key Management System
EM	Enterprise Management
ENDEX	End of Exercise
EOC	Emergency Operations Center
ESD	Enterprise Service Desk
ESDE	Enterprise Services and Data Environment
ESM/NM	Enterprise Service Management/Network Management
FAM	Functional Area Manager
FDM	Functional Data Manager
FMF	Fleet Marine Forces
FOC	Full Operational Capability
FRAGO	Fragmentary Order
GAL	Global Access List
GCC	Geographic Combatant Commanders
GCCS	Global Command and Control System
GCM	Global Information Grid (GIG) Content Management
GCT	General Classification Test
GEM	Global Information Grid (GIG) Enterprise Management
GES	Global Information Grid (GIG) Enterprise Services
GFE	Government Furnished Equipment
GIG	Global Information Grid (GIG)
GIG-BE	Global Information Grid (GIG) Bandwidth Expansion
GNA	Global Information Grid (GIG) Network Assurance
GNOSC	Global Network Operations Security Center
GOGO	Government Owned, Government Operated
GPO	Group Policy Object
HA/C/DR	High Availability, Continuity, and Disaster Recovery
HAIPE	High Assurance Internet Protocol Encryptor
HBSS	Host Base Security System
HHQ	Higher Headquarters
HQMC	Headquarters Marine Corps
HSN	High-Speed Network
HVAC	Heating, Ventilating and Air Conditioning
I&I	Impact and Implementation
I&W	Indications and Warnings
IA	Information Assurance
IAA	Information Assurance Awareness

ACRONYM	DEFINITION
IAM	Information Assurance Manager
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IC	Intelligence Community
ICS	Integrated Communications Strategy
IDS	Intrusion Detection System
INFOCON	Information Operations Condition
IOC	Initial Operation Capable
IOS	Intelligence Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPT	Integrated Product Team
Ipv6	Internet Protocol Version 6
IRM	Information Resource Manual
ISC	Information Systems Coordinator
ISM	Information Security Management
ISSO	Information Systems Security Officer
IT	Information Technology
ITI	Information Technology Instruction
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
ITSG	Information Technology Steering Group
ITSM	Information Technology Service Management
JP	Joint Publication
KM	Knowledge Management
KPI	Key Performance Indicator
LAN	Local Area Network
LMR	Land Mobile Radio
LNC	Legacy Network Consolidation
LOGCOM	Logistics Command
LRA	Local Registration Authority
M&S	Modeling and Simulation
MAC	Mission Assurance Category
MAGTF	Marine Air-Ground Task Force
MAN	Métropolitain Area Network
MARFOR	Marine Force
MCB	Marine Corps Base
MCCAP	Marine Corps Certification and Accreditation Process
MCCC	Marine Communication Control Center
MCCDC	Marine Corps Combat Development Command
MCEDS	Marine Corps Enterprise Desktop Standardization
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Marine Corps Enterprise Network

ACRONYM	DEFINITION
MCHS	Marine Corps Common Hardware Suite
MCI	Marine Corps Installation
MCIAP	Marine Corps Information Assurance Program
MCIART	Marine Corps Information Assurance Red Team
MCLB	Marine Corps Logistics Base
MCM	Marine Corps Enterprise Network (MCEN) Content Management
MCNOSC	Marine Corps Network Operations and Security Center
MCPP	Marine Corps Planning Process
MCSC	Marine Corps Systems Command
MCTSSA	Marine Corps Tactical Systems Support Activity
MCW	Marine Corps World-Wide
MCWP	Marine Corps Warfighting Publication
MD	Management Domain
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
MEM	Marine Corps Enterprise Network (MCEN) Enterprise Management
MEU	Marine Expeditionary Unit
MGCP	Media Gateway Control Protocol
Mgmt	Management
MILCON	Military Construction
MILSPEC	Military Specification
MITNOC	Marine Corps Information Technology Network Operations Center
MITSC	Marine Corps Air Ground Task Force (MAGTF) Information Technology Support Center
MNA	Marine Corps Enterprise Network (MCEN) Network Assurance
MOA	Memorandum of Agreement
MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
MROC	Marine Requirements Oversight Council
MTT/NETT	Mobile Training Team/New Equipment Training Team
NA	Network Assurance
NAS	Network Attached Storage
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NCMO	Navy Circuit Management Office
NCR	National Capital Region
ND	Network Defense
NEPA	National Environmental Policy Act
NetCOP	Network Common Operating Picture
NetOps	Network Operations

ACRONYM	DEFINITION
NGEN	Next Generation Enterprise Network
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NOSC	Network Operations and Security Center
NTP	Naval Telecommunications Procedure
O&M	Operate and Maintain
OAG	Operational Advisors Group
OI	ISO Operational Impact
OLA	Operational Level Agreement
OMPOC	Organizational Messaging Point of Contact
OpAdv	Operations Advisories
OPCON	Operational Control
OpDir	Operational Directive
OPDRS	Operational Reporting Directives Reporting System
OPFOR	Operating Force
OPLAN	Operations Plan
OPORD	Operations Order
OPTEMPO	Operating Tempo
OS	Operating System
OU	Organizational Unit
OWA	Outlook Web Access
P2T2	Polaris Prepares Tomorrow's Teachers
PAT	Port Address Translation
PCA	Permanent Change of Assignment
PCS	Permanent Change of Station
PDS	Protective Distribution System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan Of Action and Milestones
POM	Program Objective Memorandum
POP	Point of Presence
PoR	Program of Record
PP&O	Plans, Policies, and Operations
Pub	Publication
PWS	Performance Work Statements
QoS	Quality of Service
RA	Registration Authority
RACIP	Responsible Accountable Consulted Informed Participant
RDM	Release and Deployment Management
RFC	Request for Change
RFC	Request for Comment
RNOSC	Regional Network Operations and Security Center

ACRONYM	DEFINITION
ROCC	Range Operations Control Center
ROI	Return on Investment
RRS	Regional Response System
RTC	Regional Training Center
SA	Situational Awareness
SAAR	System Access Authorization Request
SACM	Service Asset and Configuration Management
SAN	Storage Area Network
SCM	Service Catalog Management
SE	Supporting Establishment
SED	Supporting Establishment Domain
SES	Senior Executive Service
SIAT	Systems Engineering Interoperability, Architecture, and Technology
SIE	Systems Integration Environment
SIM	Security Incident Management
SIPRNet	Secret Internet Protocol Router Network
SKMS	Service Knowledge Management System
SLA	Service Level Agreement
SLM	Service Level Management
SME	Subject Matter Expert
SMEPED	Secure Mobile Environment Portable Electronic Device
SNMPv3	Simple Network Management Protocol Version 3
SOA	Service Oriented Architecture
SONIC	Secure Operational Network Infrastructure Communications
SOP	Standard Operating Procedure
SORTS	Status Of Resources and Training System
SPE	Systems Planning and Engineering
SPM	Service Portfolio Management
SRB	Service Record Book
SSOG	Site Operation Guidelines
STARTEX	Start of Exercise
STIGS	Security Technical Implementation Guides
SysCon	Systems Control
T&R	Training & Readiness
TACON	Tactical Control
TBD	To Be Determined
TBMCS	Theater Battle Management Core Systems
TCCC	Theater Communication Control Center
TDMS	Tactical Defense Message System
TechCon	Technical Control
TFMS	Transportation Financial Management System
T/O&E	Table of Organization and Equipment
TMD	Tactical Management Domain

ACRONYM	DEFINITION
TRO	Tailored Response Options
TSR	Telecommunications Service Request
TTP	Tactics, Techniques, and Procedures
TTS	Trouble Ticketing System
UC	Underpinning Contract
UNAAF	Unified Action Armed Forces
UPS	Uninterruptible Power Supply
USC	United States Code
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
VIP	Very Important Person
VM	Virtual Machine
VMS	Vulnerability Management System
VoIP	Voice Over Internet Protocol
VoSIP	Voice Over Secure Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WARNORD	Warning Order
WMI	Windows Management Instrumentation
WO	Watch Officer

APPENDIX B: TERMS AND DEFINITIONS

TERM	DEFINITION
Accountable (A)	A stakeholder role or responsibility within the RACIP model. "The Buck Stops Here". The stakeholder accountable is ultimately answerable for the activity or decision. This includes "yes" or "no" authority and veto power. Only one "A" can be assigned to an action/task/function.
Active Directory (AD) Domain	An element in the logical framework of Active Directory. An AD structure is a hierarchical framework of objects. As a member of a forest, domains are identified by their DNS name structure, the namespace.
Administrative Control (ADCON)	(DoD) Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. Also called ADCON. Source: JP 1 ; JP 1-02 definition: ; ADCON - administrative control ; Source: JP 1-02
Call Center	A centralized office used for the purpose of receiving and transmitting a large volume of requests by telephone, fax, e-mail and other systems that interface directly with users. The call center does not provide any direct support for Users other than serving as the interface for service request creation. Once created, the call center turns the service request over to the service desk for assessment and action.
Certification Authority (CA)	An entity authorized by the DoD Program Management Authority (PMA) to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under this DoD Policy are performed in accordance with the requirements, representations, and warranties of that Policy. CA is an inclusive term, and includes all types of CAs. In the case of a hierarchical PKI, the CAs must be subordinate to a Root-CA (and a maximum of one intermediate CA).
Command	1. The authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. A unit or units, an organization, or an area under the command of one individual.
Command and Control (C2)	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating and controlling forces and operations in the accomplishment of the mission. Also called C2.
Command and Control System	The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the mission assigned.

TERM	DEFINITION
Command Relationships	The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control, or support.
Combatant Command (COCOM)	Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called COCOM. See also combatant command; combatant commander; operational control; tactical control. Source: JP 1 ; JP 1-02 definition: ; COCOM - combatant command (command authority) ; Source: JP 1-02
Concept of Operations (CONOPS)	A Concept of Operation is a document describing the characteristics of a proposed system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders.
Configuration Management System (CMS)	A set of tools and databases that are used to manage SIPRNet configuration data. The CMS also includes information about incidents, problems, known errors, changes, and releases; and may contain data about IT staff, suppliers, locations, Supporting and Supported Establishment organizations, customers, and users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items (CIs) and their relationships.
Consulted (C)	A stakeholder role or responsibility within the RACIP model. “In the Loop”. The consulted stakeholder (typically the subject matter expert) is to be consulted prior to a final decision or action. This is a predetermined need for two-way communication. Input from the designated position is required.
Control	Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations.
Direct Support Relationship	Direct support - (DoD) A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. Also called DS. See also close support; general support; mission; mutual support; support. Source: JP 3-09.1 direct support. A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force’s request for assistance. Also called DS. (JP 1-02) Direct support is defined as, “A mission requiring a force to support another specific force and authorizing it to answer directly the supported force’s request for assistance” (UNAAF Joint Pub 0-2). Although other types of supported/supporting relationships are possible, the direct support relationship will generally be used to define NetOps support between major commands in the Marine Corps. In order to clarify the direct support role of

TERM	DEFINITION
	organizations in NetOps, the following framework is provided.
Emergency Change	A change that must be introduced as soon as possible. e.g. resolve a major incident or implement a security patch. The change management process will normally have an abbreviated procedure for handling emergency changes.
Event	An event is any detectable or discernable occurrence that has significance for the management of the IT infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services.
Event Management	Event Management is used to define a process that helps leverage automation to manage events to become more effective and efficient In Event Management there are three paths that can be taken. **Informational:** These are events that should be logged for potential future analysis, including confirming if the service is operating as expected. **Warning:** During service design, thresholds are identified that help gauge the status of a system. When the threshold is reached, predefined parties, or notification groups, are alerted that the threshold has been reached. **Exception:** This branch is reserved for configuration items (hardware, software, or service) that are operating abnormally or have failed. Abnormal behavior criteria should be defined during service design to better understand what types of scenarios trigger what types of exception handling.
Garrison	A permanently-established facility or installation providing organic support to home-based USMC units.
General Support Relationship	General support - (DoD, NATO) 1. That support which is given to the supported force as a whole and not to any particular subdivision thereof. See also close support; direct support; mutual support; support. 2. (DoD only) A tactical artillery mission. Also called GS. See also direct support; general support-reinforcing; reinforcing.
Global Information Grid	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. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. (DoD Directive 8100.1) The GIG includes any system, equipment, software, or service that meets one or more of the following criteria: - Transmits information to, receive information from, routes information among, or interchanges information among other equipment, software, and services.Provides retention, organization, visualization, IA, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.Processes data or information for use by other equipment, software, and services.
HA/C/DR	High Availability, Continuity, and Disaster Recovery; the true measure of each would be specified in relative SLA and OLAs.

TERM	DEFINITION
Help Desk	A point of contact for users to log Incidents. A help desk is usually more technically focused than a service desk and does not provide a single point of contact for all interaction. Although the term help desk is typically synonymous with service desk, in the context of the SIPRNet COE, it is distinctively different.
Incident	An unplanned interruption to an IT service or a reduction in the quality of an IT Service. Failure of a configuration item that has not yet impacted Service is also an Incident.
Incident Management	Incident Management aims to minimize disruptions to business by restoring service operations to agreed levels as quickly as possible. Incident Management is often the first process instigated when introducing the ITIL quality framework to a Service Desk, and offers the most immediate cost reductions and quality gains.
Informed (I)	A stakeholder role or responsibility within the RACIP model. "Keep in the Picture". The informed stakeholder needs to be kept aware of the task, and needs to be informed after a decision or action is taken. They may be required to take action as a result of the outcome. It is one-way communication.
Information Resource Manual (IRM)	A document providing detailed planning and execution information.
Information Technology Architecture	Information Technology Architecture is an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals. The Department of the Navy Deputy Chief Information Officer Marine Corps has authority to develop, maintain, and facilitate the Marine Corps Information Technology Architecture and is responsible for developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for the executive agency.
Information Technology Infrastructure Library (ITIL) v3	A set of concepts and industry best practice guidance for ITSM. ITIL is owned by the United Kingdom's Office of Government Commerce (OGC) and consists of a series of publications giving guidance on the provision of quality IT Services, and on the processes and facilities needed to support them. The latest version of ITIL (v3) consists of a core set of five publications that replaces the previous version of ITIL (v2).
IT Acquisition	The function responsible for acquiring new or transforming existing Marine Corps IT resources and capacities, in accordance with the established IT Governance guidelines and policies, required by IT Operations to provide warfighting value generation to the U.S. Marine Corps.
IT Governance	The function responsible for defining, establishing, prioritizing, and measuring the enterprise IT vision, strategy, policies, resources, organizational structures and capabilities required by IT Operations to provide warfighting value generation to the U.S. Marine Corps.
IT Instruction (ITI)	A document providing detailed technical instructions, checklists, and procedures.
IT Operations	The function responsible for providing warfighting value generation to the U.S. Marine Corps operational forces through delivery of IT capabilities.
Knowledge Management (KM)	The ITSM process responsible for gathering, analyzing, storing, and sharing knowledge and information within an organization. The primary purpose of KM is to improve efficiency by reducing the need to rediscover knowledge.
Local Registration Authority (LRA)	A type of Registration Authority with responsibility for a local community.

TERM	DEFINITION
Major incident	The highest category of impact for an incident. A Major Incident results in significant disruption to the Marine Corps.
Management Domain (MD)	A term used to describe physical network architectures and the necessary permissions and controls to operate them.
Marine Corps Enterprise Network (MCEN)	The Marine Corps Enterprise Network (MCEN) is the Marine Corps' network-of-networks that provides the organic telecommunications infrastructure and interfaces required to enable the end-to-end exchange of information throughout the Marine Corps' garrison and tactical environments.
Mutual Support Relationship	That support which units render each other against an enemy, because of their assigned tasks, their position relative to each other and to the enemy, and their inherent capabilities. That support which units render each other against an enemy, because of their assigned tasks, their position relative to each other and to the enemy, and their inherent capabilities.
Net-Centricity	A robust, globally interconnected network environment (including infrastructure, systems, processes and people) in which data is shared timely and seamlessly among users, applications and platforms. It enables substantially improved military situational awareness and significantly shortened decision-making cycles.
NetCOP	The enterprise toolset used to display integrated overviews of SIPRNet status, performance, events, threats and vulnerabilities ranging from high level global views down to more granular views of each region, base, LAN, command, and end device. The primary purpose of NetCOP is to present IT service management personnel Situational Awareness (SA) of SIPRNet services and to improve the quality and timeliness of collaborative decision-making.
NetOps C2	Given the nature of regionalized NetOps, many NetOps activities may not originate from a single command authority; therefore, C2 processes are needed to ensure unity of effort. NetOps C2 activities support the global integration of NetOps, across widely dispersed network operations centers, to operate and defend the network in a manner consistent with operational priorities across the range of military and business operations.
NetOps Tasking and Reporting Framework	A term used to describe the structure used within NetOps that falls outside of the operational chain of command. It represents the functional chain of command for NetOps.
Network Assurance	GIG Enterprise Management (GEM), GIG Net Assurance (GNA), and GIG Content Management (GCM) functions shall be operationally and technically integrated to ensure simultaneous and effective monitoring, management, and security of the enterprise.
Normal Change	A new or non-standard change for which implementation time allows for handling via the full change management process.
Operating Forces	Those forces whose primary missions are to participate in combat and the integral supporting elements thereof.
Operational Control (OPCON)	(DoD) Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to

TERM	DEFINITION
	accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. See also combatant command; combatant command (command authority); tactical control.
Operational Level Agreement (OLA)	OLAs are agreements between the Service Provider and other elements of the organization in support of the Service Provider's IT service delivery mission. They define the material and/or services that the supporting organization provides and the terms in which they provide them. In effect, these are the traditional Memoranda of Agreement (MOA) that the Marine Corps has long used but are specific to IT and placed in terms of the Service Level Management process . As there are multiple service providing organizations, and none are self sufficient, OLAs become critical instruments for effective service delivery both within the regions and between the enterprise and regional NetOps layers.
Participant (P)	A stakeholder role or responsibility within the RACIP model. "The Assistant". The participant stakeholder assists the responsible (R) stakeholder in actually performing the task. There may be more than one "P".
Problem	A state, identified from incidents, which indicates an error in the IT infrastructure. A problem remains in this state until a cause is found. Note that a Known Error is a Problem for which the cause is found and is often related to a fault with a configuration item (CI) or a number of CIs in the IT infrastructure.
Problem Management	Problem Management investigates the underlying cause of incidents, and aims to prevent incidents of a similar nature from recurring. By removing errors, which often requires a structural change to the IT infrastructure, the number of incidents can be reduced over time.
Public Key Infrastructure (PKI)	A combination of hardware, software, policies, and procedures, as well as, the ability to authenticate, protect, digitally sign, and when necessary, encrypt electronic mail (e-mail) and documents. PKI verifies identities through the use of digital signatures and certificates.
Registration Authority (RA)	An entity that enters into an agreement with a CA to collect and verify Subscriber identity and information, which is to be entered into public key certificates. The RA must perform its functions in accordance with a Certification Practice Statement (CPS) approved by the Program Management Authority (PMA).
Responsible (R)	A stakeholder role or responsibility within the RACIP model. "The Doer". The responsible stakeholder actually completes the task. The "doer" is responsible for action/implementation. The degree of responsibility is determined by the "Accountable (A)" individual.
Service	A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

TERM	DEFINITION
Service Command	A term used to describe directive authority for all types of operations falling outside of other formally established command relationships, such as USSTRATCOM's OPCON authority for CND. It includes the authorities necessary for the Marine Corps to install, operate, and maintain the SIPRNet as part of its Title 10 man, train, and equip responsibilities.
Service Desk	The single point of contact between the Service Provider and the users. A typical service desk manages Incidents and service requests, and also handles communication with the users. The service desk differs from a call center, contact center or a Help desk by offering a more broad and user-centric approach, which seeks to provide a user with an informed single point of contact for all of their IT requirements. A service desk seeks to facilitate the integration of business processes into the Service Management infrastructure. In addition to actively monitoring and owning Incidents and user questions, and providing the communications channel for other Service Management disciplines with the user community, a service desk also provides an interface for other activities such as customer change requests, third parties (e.g. maintenance contracts), and software licensing.
Service Knowledge Management System (SKMS)	A set of tools and databases that are used to manage knowledge and information. The SKMS includes the Configuration Management System (CMS), as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that NetOps organizations need to manage the full lifecycle of IT services.
Service Level Agreement (SLA)	Agreements between the service provider and its customers. They cover details of the service(s) to be provided (a single SLA may cover multiple services or customers), document Service Level Targets, and detail the responsibilities and commitments of both the service provider and customer. SLAs will be negotiated within the SLM process.
Service Level Management	Service Level Management (SLM) determines appropriate IT service targets, ensures that an agreed level of service is provided for all current IT services, and that future services are delivered to agreed targets. SLM is the process of negotiating, defining, measuring, managing, and improving the quality of IT services at an acceptable cost. SLM ensures that the IT services required by end users are continuously maintained and improved. This is accomplished through the establishment and enforcement of SLAs.
Service Support Centers	A generic term used to refer to general support organizations including but not limited to data centers, operation centers, and the EITC. Service support center is not a title.
Situational Awareness	The application of Information Age technology to military C2 resulting in an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.
Standard Change	A pre-approved change that is low risk, relatively common and follows a procedure or work instruction. e.g. password reset or provision of standard equipment to a new employee. Request for changes are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a service request.
Supporting Establishment Management Domain	An organizational hierarchy that is associated with the entire IT infrastructure within the B/S and non-deployable environment. This single hierarchy is used for NetOps tasking and reporting as well as to provide service for the garrison environment.

TERM	DEFINITION
Systems Control (SysCon)	The systems control (SysCon) performs current operations functions for communications operations. The SysCon is established by the operations officer of each communications unit to maintain current information on availability and operational readiness of CIS, set priorities and resolve conflicts. SysCon personnel perform their duties in an appropriate facility in the vicinity of the supported command post. The SysCon receives direction from the Systems Planning and Engineering section. The SysCon coordinates directly with senior, subordinate, and adjacent SysCons as required. SysCon personnel must have the technical expertise and experience to coordinate resolution of complex communications problems. (MCWP 3-40.3 Jan 2010)
Tactical Control (TACON)	(DoD) Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. Also called TACON. See also combatant command; combatant command (command authority); operational control.
Tactical Management Domain	The various organizational hierarchies associated with deployed networks inherent to the Operating Forces. These Tactical Management Domains exist when forces (MEFs, MEUs, and MEBs) deploy under the control of a COCOM, and when they exercise and operate in temporary tactical environments. When deployed, IT services transition into the tactical MDs. NetOps tasking and reporting for this separate tactical enclave also changes.
Technical Control (TechCon)	TechCon is the means of exercising centralized technical supervision over the installation, operation, and maintenance of the circuits and systems employed by the MAGTF. The installation of each system is controlled by a TechCon facility. TechCon provides centralized technical supervision over the installation, operation, and maintenance of single channel radio, wire, multichannel and data communications systems (including video). TechCon functions are performed from specially designed TechCon facilities, the network operations center, maintenance facilities, and communications centers, when established. The TechCon facilities provide a means to conduct and coordinate circuit troubleshooting and restoration. The size and scope of the TechCon facilities are driven by the size of the communications organization and types of services being provided. TechCon personnel must have the technical expertise and experience to resolve complex communications problems. (MCWP 3-40.3 Jan 2010)
VIP	Very Important Persons (VIPs) are defined across the Marine Corps SIPRNet as 'General Officers or their Senior Executive Service (SES) civilian equivalents'.

APPENDIX C: REFERENCES

A. Joint Publication 0-2, Unified Action Armed Forces (UNAAF), 10 July 2001, http://www.dtic.mil/doctrine/jel/new_pubs/jp0_2.pdf

B. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (As Amended Through 17 October 2008), http://www.fas.org/irp/doddir/dod/jp1_02.pdf

C. Joint Publication 6-0, Joint Communications System, 20 March 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp6_0.pdf

D. Title 10 ("Armed Forces"), United States Code, section 164, Subtitle A. General Military Law, Part I. Organizations and General Military Powers, Chapter 6. Combatant Commands, 11/16/2007, http://tigs-online.ignet.army.mil/tigu_online/CCJIGC/10_USC_164.pdf

E. Communications Tasking Orders (CTOs), Joint Task Force Global Network Operations (JTF-GNO), https://www.jtfgno.mil/operations/cto/2009/index.htm

F. Fragmentary Orders (FRAGOs), JTF-GNO, https://www.jtfgno.mil/operations/frago/2009/index.htm

G. Information Assurance Vulnerability Management (IAVM) Notices, Information Assurance Vulnerability Advisories (IAVAs), JTF-GNO, https://www.jtfgno.mil/iavm/index.html

H. Security Technical Implementation Guides (STIGS) and Supporting Documents, Defense Information Systems Agency (DISA), http://iase.disa.mil/stigs/

I. Department of Defense (DoD) Instruction 8500.2, Information Assurance (IA) Implementation, February 6, 2003, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

J. JROCM 134-01, "Capstone Requirements Document Global Information Grid," 30 August 2001, Available from CRD Executive Agent, U.S. Joint Forces Command (ATTN: J61)

K. DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9,1996, http://www.dtic.mil/whs/directives/corres/pdf/523009p.pdf

L. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E, Information Assurance (IA) and Computer Network Defense (CND), 15 August 2007, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

M. Integrated Communication Strategy (ICS)

N. Information Technology Instructions (ITIs)

O. Tactics, Techniques, and Procedures (TTPs)

P. MCWP 3-40.3 (Formerly MCWP 6-22), Communications and Information Systems, MCCDC (C 42), 10 July 2001, https://www.doctrine.usmc.mil/restrictedpubs/w3403.pdf

Q. DoDI 8410.02, NetOps for the Global Information Grid (GIG), December 19, 2008, http://www.fas.org/irp/doddir/dod/i8410_02.pdf

R. Secretary of Defense Memorandum, "Assignment and Delegation Authority to Director, Defense Information Systems Agency (DISA)," June 18, 2004

S. DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007, http://www.diacap.net/images/851001p.pdf

T. DoDD 8100.1, Global Information Grid (GIG) Overarching Policy, November 21, 2003, http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf

U. DoDD 8500.01E, Information Assurance (IA), April 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

V. MCO 5239.2, Marine Corps Information Assurance Program (MCIAP), 18 Nov 02, http://www.marines.mil/news/publications/Documents/MCO%205239.2.pdf

W. MCO 3900.17, The Marine Corps Urgent Needs Process (UNP) and the Urgent Universal Need Statement (Urgent UNS), Oct 17, 2008, http://www.marines.mil/news/publications/Documents/MCO%203900.17.pdf

X. MCO 3900.15B, Marine Corps Expeditionary Force Development System (EFDS), 10 March 2008, http://www.marines.mil/news/publications/Documents/MCO%203900.15B.pdf

Y. HQMC MSG 002-08, SIPRNet Way Ahead RNOSC, MSGID: DTG 021903Z JUL 08

Z. HQMC MSG 003-08, SIPRNet Way Ahead MITSC, MSGID: DTG 022047Z JUL 08

AA. USSTRATCOM Joint Concept of Operations for Global Information Grid NetOps

APPENDIX D: DOD PKI SIPRNET IMPLEMENTATION

DoD PKI will implement a hardware token issuance capability on the SIPRNet began with a pilot implementation in 4Qtr FY09 and is targeting IOC in 3rd Qtr FY10. The initial hardware token will be in a smartcard form factor. The issuance infrastructure will be centrally configured and maintained by DISA. Issuance of hardware tokens will be managed by each service using the DoD PKI provided certificate management system. Issuance of SIPRNet hardware tokens will be accomplished either centrally by the MCNOSC RA Operations Section or by MCNOSC RA Personnel located at each MITSC/B/S's. The DoD PKI SIPRNet hardware token will be used for network access, access to network resources, such as SIPRNet private web servers, and the digital signature and/or encryption of SIPRNet email. Issuance of SIPRNet Hardware Tokens will be in accordance with DoD Certificate Policy and the USMC RA Certificate Practice Statement.

CERTIFICATE VALIDATION INFRASTRUCTURE (CVI). Critical to the use of PKI certificates on the network is the ability to check the validity of a certificate. DoD PKI Certificate Authorities publish certificate revocation lists on a regular basis. MCNOSC PKI will manage the consumption of DoD SIPRNet CRL's centrally at the MCNOSC and ALTNOSC. CVI Responders, located at the MCNOSC and ALTNOSC will process the CRL's and push validation information to CVI Repeaters located at each MITSC. Relying parties (clients, servers, applications) located at MITSC's will be configured to use local MITSC repeaters for certificate validation status. The attached diagram of the USMC SIPRNet CVI depicts the architecture as it pertains to the SIPRNet MCEN.

MICROSOFT CERTIFICATE AUTHORITY (CA) INFRASTRUCTURE. At this time, the DoD PKI does not have the ability to autonomously issue Microsoft domain controller certificates. Domain controller certificates are required in order to enable a Microsoft network for cryptographic logon. MCNOSC PKI will initiate a Microsoft Root CA and several Subordinate CA's to meet this requirement. The Root CA and Sub-CA's will be maintained at both the MCNOSC and ALTNOSC and will be available to MITSC's for the issuance of Domain Controller Certificates. At a point in time when the DoD PKI has the ability to issue Domain Controller Certificates autonomously across the GIG the MCNOSC PKI will migrate to that solution.

CLIENT CONFIGURATION. MCNOSC PKI will provide the necessary hardware token reader, reader middleware and validation software with the proper configurations to enable the client to use the SIPRNet Hardware token for access to the network, network resources and email signature and/or encryption. Configuration of the validation software will be controlled by the MCNOSC PKI with specific primary and secondary validation nodes configured based on MITSC location. This same hardware, middleware and software will be available for configuration on servers to allow for the use of hardware tokens vice username/password for system administrators.

REGISTRATION AUTHORITY. MCNOSC PKI Section will be the RA for the Marine Corps. Per the Marine Corps RA Certificate Practice Statement (CPS) RA Operations at the MCNOSC will be responsible for the issuance of certificates, revocation of certificates, directory entries, SIPRNet Hardware Token inventory, management and distribution as well as Tier 3 support to the SIPRNet community.

APPENDIX E: PLANNING

Planning establishes procedures and parameters for contingencies which could be done beforehand or in response to actual and potential events/incidents. It also establishes levels of operational control and delegated authorities for each organization involved in a specific operation or theater of action. Finally, planning evaluates current and past performance to gain lessons learned and to improve the planning process for future operations. Importantly, planning always requires close coordination between the operator (end-user) and the planner in order to maintain clarity, efficiency and effectiveness during the transition from planning to execution when implementing solutions to existing capability gaps on the SIPRNet.

NetOps planning is an ongoing process that occurs at the enterprise, regional, and local levels in order to meet operational and technical requirements. It is a form of adaptive planning (defined in Joint Pub 5-0 as "the joint capability to create and revise plans rapidly and systematically, as circumstances require.") and includes those actions taken to coordinate and planning and execution of daily operations for accomplishing assigned missions and tasks, as well as conduct future planning, training, and exercise participation to ensure Marine Corps readiness and improved NetOps capabilities to meet future and current Joint operational requirements.

PLANNING RESPONSIBILITIES

Strategic

Strategic planning regarding the Marine Corps Garrison SIPRNet is conducted at or above the HQMC level (including Joint Staff, DISA, and USCYBERCOM levels.) It sets the vision and goals for the Marine Corps and DoD classified networks. Strategic planning provides organizational focus and establishes priorities. Strategic plans for the SIPRNet are generally developed by IT Governance organizations, most notably HQMC C4.

Operational

Operational planning has the function of translating strategic objectives into a series of operational plans, objectives and capabilities for the Marine Corps. Operational plans for the SIPRNet are generally developed by the senior IT operational organizations, including the MCNOSC, MARFORCYBERCOM and HQMC C4.

Tactical

Tactical planning is focused almost exclusively on achieving specific tangible objectives as set forth in planning guidance from higher. The output of tactical planning efforts may take the form of SOPs, TTPs, or ITIs. Tactical plans for the SIPRNet are generally developed by IT operational organizations, including the MCNOSC, RNOSC, and MITSCs.

TYPES OF PLANNING

SIPRNet planning is accomplished through Mission Planning, as described in the Marine Corps Planning Guide and The DOTMLPF analysis processes. Both planning processes support NetOps and are integrated with IT Services Management – in particular Change Management.

MISSION PLANNING

Marine Corps Warfighting Publication (MCWP) 5-1, Marine Corps Planning Process (MCPP), describes a planning process that supports decision-making by the commander. It is also a vehicle that conveys the commander's decisions to his subordinates. It is applicable to all echelons of command and across all ranges of military operations. This MCPP complements joint deliberate and crisis action planning and the naval planning process. It is a responsive and flexible process that can adapt to the needs of any size unit and adjust to any timetable. The MCPP embodies our maneuver warfare doctrine with its tenets of top-down planning, single-battle concept, and integrated planning in order to generate and maintain tempo.

The planning process focuses primarily on the planning and execution of missions. This planning is an essential and significant part of C2 and recognizes the centrality of the commander in the planning process. Through the RNOSC/MITSC structure, it uses mission planning processes to prepare for tasks in support of Higher Headquarters (HHQ) direction, such as a CTO or WARNORD. It fully considers operational impact and risk in the development of NetOps Courses of Action (COA). This planning process, as detailed in MCWP 5-1, is comprised of six integrated steps:

Step 1: Mission Analysis.
Step 2: COA Development.
Step 3: COA Analysis.
Step 4: COA Comparison/Decision
Step 5: Orders Development.
Step 6: Transition.

DOTMLPF Analysis

Doctrine, Organization, Training, Material, Leadership & Education, Personnel, and Facilities (DOTMLPF) is a systematic approach to program development and review. It identifies key program elements, all interconnected that must be addressed. Failure to address any one typically leads to significant problems in program design, completion, or response. The system is based on many lessons learned within the military. The seven pillars of DOTMLPF are explained below.

Doctrine

The Doctrine element addresses the way we fight. It includes those concepts, principles, policies, tactics, techniques, practices, and procedures, which are essential in organizing, training, equipping and employing tactical and supporting units. Typical questions/concerns: determine if doctrine exists; determine if doctrine is current; identify doctrinal gaps; review coalition doctrine; joint publication synchronization; develop Plan of Action & Milestones (POA&Ms) for all doctrinal changes required; etc.

Table 44: Roles and Responsibilities Table for Doctrine

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Update the USMC strategy and policy as required.		RA						
Provide SIPRNet operational guidance.		RA						
Develop and maintain ITIs for operators related to MITSC hardware, software, and operations.	RA							
Lead the MCEDS effort to develop procurement strategy for standard software load and application license support.			RA					
Coordinate the development of required PoR documentation.			RA					
Develop desktop and server policies and procedures.	R		A					

Organization

The Organization element addresses how we organize to fight and fulfill missions. Typical questions/concerns: determine OPLAN impacts (with DC, PP&O); develop mission statement; develop T/O&E; determine "Mirror Imaging" impacts; determine Marine Corps impact; define IOC/FOC; implement T/O&E into (Transportation Financial Management System (TFMS); develop 5400 bulletin; determine command relationships; identify recommended compensation; determine requirement to reconstitute capabilities removed from Fleet Marine Forces (FMF); determine additional maintenance/support requirements; determine joint requirement impact; determine Impact and Implementation (I&I) impacts; determine new unit names/locations; determine manning precedence level to be assigned; develop POA&M for all organizational actions required; etc.

Table 45: Roles and Responsibilities Table for Organization

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Develop/Modify Table of Organizations (T/O)		RA						
Identify organization framework/construct		RA						
Determine OPLAN impacts (with DC, PP&O)								
Develop mission statement								

Training

The Training element addresses how we prepare to fight tactically; basic training to advanced training, various types of unit training, joint exercises, etc. Typical questions/concerns: Determine all new manpower training requirements [including assess training throughput; determine school seat requirements; determine instructor requirements (USMC & external)]; develop Training and Readiness (T&R) manual; develop SOPs; determine inter-service training necessary; review inter-service training agreements; develop Military Occupational Specialty (MOS) road-maps; determine Mobile Training Team / New Equipment Training Team (MTT/NETT) requirements; determine MOS manual impacts; determine MOS related certification requirements; determine incidental certification requirements; determine formal school requirements; etc.

Table 46: Roles and Responsibilities Table for Training

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Coordinate the development and implementation of training related to the operation and defense of the SIPRNet		RA						
Coordinate the training and certification of ESD and touch labor personnel at the enterprise, regional, and local level in troubleshooting and ITSM procedures	R	I	A		P	P		
Identify training requirements	C	RA	P	C	C	C		C
Support changes/additions to training (school houses)		RA						

Materiel

The Materiel element addresses all material components including the physical hardware, software and peripheral equipment necessary to equip our forces so units can operate effectively. Typical questions/concerns: determine sourcing plan for equipment [including determine cost and development appropriate budget submissions; prioritize sourcing with other sourcing efforts; develop procurement plans and estimates of supportability (timeline); develop new equipment fielding plans; develop redistribution plans]; develop disposition plan for equipment currently on hand by units that may be used as compensation for this activation; determine Approved Acquisition Objective (AAO) impacts; determine intermediate level impacts; determine new combat development issues; determine impacts on maintenance/readiness; determine equipment life cycle issues; determine impact on classes of supply; develop Status of Resources and Training System (SORTS) assessment; develop POA&M for all material actions required; and provide monthly status reports for all actions.

Table 47: Roles and Responsibilities Table for Materiel

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Program Objective Memorandum (POM) for the funding of SIPRNet requirements to sustain the SIPRNet for all validated materiel requirements.		A	R					
Engineer or implement technical solutions for enterprise network initiatives.			RA					
Provide assistance in the transition and review of new SIPRNet related technologies.	R		A					

Leadership and Education

The Leadership and Education element addresses how we prepare our leaders to lead the fight from squad leader to 4-star general; professional development. Typical questions/concerns: determine communication plan; determine command relationships; develop service letter of agreement between USMC and others (if any) [including C2 relationships and Memorandums of Agreement / Understanding (MOAs/MOUs)]; determine Communication Security (COMSEC) Material System/Electronic Key Management System (EKMS) requirements; develop change management plan; develop POA&M for all leadership actions required; etc.

Table 48: Roles and Responsibilities Table for Leadership

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Provide top-down advocacy for employment of ITSM use in the USMC.		RA						

Personnel

The Personnel element addresses the availability of qualified personnel for peacetime, wartime, and various contingency IT operations. Typical questions/concerns: determine operations tempo and personnel tempo impacts; determine accessions numbers; develop staffing plan to achieve IOC and FOC requirements; determine recruiting impact; determine reserve impacts; determine command screening issues; determine E8/E9 screening issues; MOS assignment and conversion policy; maintenance and support MOSs (also with organization); generate grade shaping assessment; determine Service Record Book (SRB) and Lateral Move impacts; determine Armed Services Vocational Aptitude Battery (ASVAB) and General Classification Test (GCT) needs impact; identify Polaris Prepares Tomorrow's Teachers (P2T2) impact; determine unit precedence impact (ID bill payers); determine legislative constraint impact; develop SORTS assessment; determine DON impact; determine civilian impact; etc.

Table 49: Roles and Responsibilities Table for Personnel

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Coordinate the identification, movement, reassignment or addition of personnel (table of organization structure) to support the operation of the USMC SIPRNet.	R	A		P				

Facilities

The Facilities element addresses real property; installations and industrial facilities that support our forces. Typical questions/concerns: conduct facilities assessment; determine Military Construction (MILCON) impacts and timeframe; determine environmental impact; determine National Environmental Policy Act (NEPA) requirements; determine building conversion impacts; determine training/schoolhouse/billeting impact; determine base/facilities support impact; determine Regional Training Center (RTC) impact; develop an integrated facilities plan that will meet IOC/FOC projected dates; develop facilities addendum to service letter of agreement between USMC and others (if any); develop POAM for all facility actions required; etc.

Table 50: Roles and Responsibilities Table for Facilities

Legend: (See Appendix B for definitions) Responsible (R) Accountable (A) Consulted (C) Informed (I) Participant (P)	MCNOSC	HQMC (C4 or I&L)	MCSC	RNOSC	MITSC	B/S	Application Owner	Tenant/Supported Cmd
Submit MILCON/Facility projects via chain of command for projects or funding requests.	RA			CP	P			
Approve MILCON/Facilities projects		RA						
Ensure MITSC facilities have adequate power, HVAC, floor space, and production rack space.		A	R		P			
Coordinate with B/S G6s to ensure adequate facilities are available to support SIPRNet.				A	R	C		

OPERATIONAL IMPACT AND RISK ASSESSMENTS

The concepts of MAC, risk assessment, and operational impact are crucial to the planning for and execution of IT services, in particular NetOps, as the framework for operating and defending DoD and Marine Corps networks. Visibility and SA through the RNOSC/MITSC structure is a crucial component needed by Commanders at all levels to determine the impact of NetOps events on their missions and to direct necessary action to ensure mission success. This is especially true for NetOps commanders charged with operating and defending the network under command of USSTRATCOM and USCYBERCOM. When dealing with IT systems, it's helpful to understand the relationships between four key components: threats, vulnerabilities, assets, and countermeasures.

- Threats exploit vulnerabilities and damage asset(s)
- Countermeasures mitigate vulnerabilities and may help in mitigating a threat

Mission Criticality Assessments (See section 4.3.6.2)

Risk Assessments

Risk Assessment is a process which helps analyze threats to and vulnerabilities of an IT system, and the potential impact that the loss of information or capabilities of a system would have on a national security. This data is then used as a basis for identifying appropriate and cost-effective measures. It is concerned with gathering information on what the vulnerabilities are and making appropriate decisions about managing this risk. Risks are often framed in a mathematical expression, Risk = Threat x Vulnerability x Opportunity.

Risk Assessments - Methodology

The basic steps in conducting a risk assessment are:

- Identify system assets and their corresponding MAC. The MAC level is often used as a basis for calculating threat risks and countermeasure priorities.
- Identify system vulnerabilities. This requires a detailed understanding of the system's functionality, architecture, software, and interfaces.
- Predict (even the most hypothetical) threat scenarios.
- Evaluate threat probability and damage in order to be able to prioritize the corresponding countermeasures.

Operational Impact Assessments

Operational Impact (OI) refers to detrimental effects to an organization's ability to perform its mission. This may include direct and/or indirect impacts that diminish or incapacitate system or network capabilities, the compromise and/or loss of mission critical data or the temporary or permanent loss of mission critical applications or systems. Refer to CJCSM 6510.01 for examples.

Operational Impact Assessments - Methodology

Operational Impact Assessments are conducted by evaluating the loss of one or more systems due to an incident or event. The MAC level forms the basis for determining the criticality of the system(s). In general, any event or incident involving a MAC I system is extremely likely to have high operational impact. Additional factors such as anticipated duration of the event or incident, availability of other systems or spares, timing, may influence the operational impact assessment.

APPENDIX F: OPDIRS & OPADV STANDARD FORMATS

OpDir Format

```
*************** UNCLASSIFIED// ***************
Subject: MCEN OPERATIONAL DIRECTIVE ###-YY, DECSRIPTION
Originator: MCNOSC QUANTICO VA(UC)
DTG: DDTTTTZ Mmm YY
Precedence: ROUTINE
DAC: General
To: AL NETOPS G-6(UC)
Cc: MCNOSC QUANTICO VA(UC)
Attachments:
--------------------------------------------------

UNCLASSIFIED//
REF/A/ (U/FOUO)//
REF/B/MSGID://
POC/OPERATIONS CENTER/WATCH OFFICER/MCNOSC OPERATIONS/-/DSN: 278-
5300/COMM: 703-784-5300/E-MAIL: OPERATIONSCENTER@MCNOSC.USMC.MIL//
NARR/ REF A IS //
1.  PURPOSE.
3.  ACTION.
A.  ACKNOWLEDGE RECEIPT OF THIS OPDIR WITHIN XX HOURS OF RECEIPT PER
REF ABC.
B.  IAMS:
(1)
(2)
(3)
(4)
C.  COORDINATING INSTRUCTIONS.
(1)
D.  FOR ADDITIONAL INFORMATION REGARDING THIS OR OTHER MCEN OPERATIONAL
DIRECTIVES OR ADVISORIES, CONTACT THE MCNOSC WATCH OFFICER AT DSN: 278-
5300. COM: (703)-784-5300 OR VIA E-MAIL AT MCNOSCWO@MCNOSC.USMC.MIL.//

_____

Details:

TO Addressees
DOD, USMC, ADDRESS LISTS, AL NETOPS G-6, AL NETOPS G-6(UC)
CC/Info Addressees
DOD, USMC, ORGANIZATIONS, TENANT, MCNOSC QUANTICO VA(UC)
Originator-DN: DOD, USMC, ORGANIZATIONS, TENANT, MCNOSC QUANTICO VA(UC)
ClassificationMark-ACP120: UNCLASSIFIED//
PrivacyMark-ACP120: PRIVACY MARK UNDEFINED
Precedence Copy: ROUTINE
Recipient-DN: DOD, USMC, ORGANIZATIONS, TENANT, MCNOSC QUANTICO VA(UC)
772-Copy-Recipient-DN: /C=US/O=U.S.
GOVERNMENT/OU=DoD/OU=USMC/OU=ORGANIZATIONS/L=MCB QUANTICO
VA/OU=TENANT/OU=MCNOSC QUANTICO VA(UC)
```

OpAdv Format

```
*************** UNCLASSIFIED// ***************
Subject: MCEN OPERATIONAL ADVISORY ###-YY, NOTIFICATION
Originator: MCNOSC QUANTICO VA(UC)
DTG: DDTTTTZ Mmm YY
Precedence: ROUTINE
DAC: General
To: AL NETOPS NOTIFICATION(UC), AL NETOPS G-6(UC)
Cc: MCNOSC QUANTICO VA(UC)
-------------------------------------------------

UNCLASSIFIED//
UNCLASSIFIED//
MSGID/GENADMIN/MCNOSC QUANTICO VA//
SUBJ/MCEN OPERATIONAL ADVISORY 094-09, NOTIFICATION//
POC/OPERATIONS CENTER/WATCH OFFICER/MCNOSC OPERATIONS/-/TEL:DSN 278-
5300/TEL:COMM 703-784-5300//
GENTEXT/REMARKS/1. PURPOSE.
2. ACTION.
3. ANY QUESTIONS REGARDING THIS NOTIFICATION SHOULD BE DIRECTED TO THE
MCNOSC OPERATIONS CENTER WATCH OFFICER AT DSN: 278-5300, COMM:703-784-
5300, OR VIA E-MAIL: OPERATIONSCENTER@MCNOSC.USMC.MIL//


_____________________________________________

Details:

TO Addressees
DOD, USMC, ADDRESS LISTS, AL NETOPS NOTIFICATION, AL NETOPS
NOTIFICATION(UC)
DOD, USMC, ADDRESS LISTS, AL NETOPS G-6, AL NETOPS G-6(UC)
CC/Info Addressees
DOD, USMC, ORGANIZATIONS, TENANT, MCNOSC QUANTICO VA(UC)
Originator-DN: DoD, USMC, ORGANIZATIONS, TENANT, MCNOSC QUANTICO VA(UC)
ClassificationMark-ACP120: UNCLASSIFIED//
PrivacyMark-ACP120: PRIVACY MARK UNDEFINED
Precedence Copy: ROUTINE
Recipient-DN: DOD, USMC, ORGANIZATIONS, TENANT, MCNOSC QUANTICO VA(UC)
772-Copy-Recipient-DN: /C=US/O=U.S.
GOVERNMENT/OU=DoD/OU=USMC/OU=ORGANIZATIONS/L=MCB QUANTICO
VA/OU=TENANT/OU=MCNOSC QUANTICO VA(UC)
```

APPENDIX G: ORGANIZATIONS

Note: NetOps Reporting Chain will follow C2 Organization Hierarchy below the MEF level in each region's MITSC, with the exception of:

1) Reserve units located on Marine Corps installations supported by non-res MITSCs. Those units fall under the supporting MITSC for NetOps reporting.
2) Tenant commands in the DC area. Demarcation point in the Metro DC area will sit at the beltway. Those organizations located within the beltway will be serviced and report through MITSC HQMC. Those organizations located outside of the beltway will be serviced and report through MITSC NCR, regardless of their operational C2 organizational hierarchy.

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
10th Marine Regiment	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 10th Marine Regiment
11th Marine Expeditionary Unit (MEU)	Camp Pendleton, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 11th Marine Expeditionary Unit
11th Marine Regiment	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 11th Marine Regiment
12th Marine Corps District (MCD)	San Diego, CA	CG MCRC	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District
12th Marine Regiment	Okinawa, Japan	CG 3 MARDIV	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 12th Marine Regiment
13th Marine Expeditionary Unit (MEU)	Camp Pendleton, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 13th Marine Expeditionary Unit
14th Marine Regiment	Fort Worth, TX	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment
15th Marine Expeditionary Unit (MEU)	Camp Pendleton, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 15th Marine Expeditionary Unit
1st Amphibious Assault Vehicle (AAV) Company	Okinawa, Japan	CO CAB	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > Combat Assault Battalion > 1st Amphibious Assault Vehicle Company
1st Battalion, 1st Marines (1/1)	Camp Pendleton, CA	CO 1st Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Marine Regiment > 1st Battalion, 1st Marines
1st Battalion, 10th Marines (1/10)	Camp Lejeune, NC	CO 10th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 10th Marine Regiment > 1st Battalion, 10th Marines
1st Battalion, 11th Marines (1/11)	Camp Pendleton, CA	CO 11th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 11th Marine Regiment > 1st Battalion, 11th Marines
1st Battalion, 12th Marines (1/12)	Kaneohe Bay, HI	CO 3d Marines	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 3rd Marine Regiment > 1st Battalion, 12th Marines
1st Battalion, 14th Marines (1/14)	Alameda, CA	CO 14th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 1st Battalion, 14th Marines
1st Battalion, 23rd Marines (1/23)	Houston, TX	CO 23rd Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 1st Battalion, 23rd Marines
1st Battalion, 24th Marines (1/24)	Selfridge Air National Guard Base, MI	CO 24th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 1st Battalion, 24th Marines

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
1st Battalion, 25th Marines (1/25)	Fort Devens, MA	CO 25th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 1st Battalion, 25th Marines
1st Battalion, 2nd Marines (1/2)	Camp Lejeune, NC	CO 2d Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Marine Regiment > 1st Battalion, 2nd Marines
1st Battalion, 3rd Marines (1/3)	Kaneohe Bay, HI	CO 3d Marines	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 3rd Marine Regiment > 1st Battalion, 3rd Marines
1st Battalion, 4th Marines (1/4)	Camp Pendleton, CA	CO 1st Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Marine Regiment > 1st Battalion, 4th Marines
1st Battalion, 5th Marines (1/5)	Camp Pendleton, CA	CO 5th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 5th Marine Regiment > 1st Battalion, 5th Marines
1st Battalion, 6th Marines (1/6)	Camp Lejeune, NC	CO 6th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 6th Marine Regiment > 1st Battalion, 6th Marines
1st Battalion, 7th Marines (1/7)	29 Palms, CA	CO 7th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 7th Marine Regiment > 1st Battalion, 7th Marines
1st Battalion, 8th Marines (1/8)	Camp Lejeune, NC	CO 8th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 8th Marine Regiment > 1st Battalion, 8th Marines
1st Battalion, 9th Marines (1/9)	Camp Lejeune, NC	CO 6th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 6th Marine Regiment > 1st Battalion, 9th Marines
1st Combat Engineer Battalion (1st CEB BN)	Camp Pendleton, CA	CG 1 MARDIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Combat Engineer Bn
1st Combat Engineer Company (1st CEB Co)	Okinawa, Japan	CO CAB	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > Combat Assault Battalion > 1st Combat Engineer Company
1st Dental Battalion (1st Dent BN)	Camp Pendleton, CA	CG 1 MLG	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > 1st Dental Battalion
1st Direct Support Platoon, Motor Transport Maintenance Company (MTM Co), 4th MAINT BN	Dyess Air Force Base, Abilene, TX	CO MTM Co	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Maintenance Battalion > Motor Transport Maintenance Company > 1st Direct Support Platoon
1st Division Reconnaissance Company	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Division Reconnaissance Company
1st Force Reconnaissance Company	Camp Pendleton, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Force Reconnaissance Company
1st Light Armored Recon Company	Camp Pendleton, CA	CO CAB	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > Combat Assault Battalion > 1st Light Armored Recon Company
1st Light Armored Reconnaissance Battalion	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Light Armored Reconnaissance Battalion
1st Maintenance Battalion	Camp Pendleton, CA	CO CLR-15	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > Combat Logistics Regiment 15 > 1st Maintenance Battalion
1st Marine Aircraft Wing (1 MAW)	Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing
1st Marine Corps District (MCD)	Brooklyn, NY	CG MCRC	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District
1st Marine Division (MARDIV)	Camp Pendleton, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division
1st Marine Expeditionary Brigade (MEB)	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Expeditionary Brigade

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
1st Marine Logistics Group (MLG)	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group
1st Marine Regiment	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Marine Regiment
1st Marine Special Operations Battalion	Camp Lejeune, NC	CG MARSOC	RNOSC-LANT	MITSC East	U.S. Marine Corps Forces, Special Operations Command > 1st Marine Special Operations Battalion
1st Medical Battalion	Camp Pendleton, CA	CO CLR-15	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > Combat Logistics Regiment 15 > 1st Medical Battalion
1st Stinger Battery	MCAS Futenma, Okinawa, Japan	CO MACG-18	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18 > 1st Stinger Battery
1st Supply Battalion	Camp Pendleton, CA	CO CLR-15	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > Combat Logistics Regiment 15 > 1st Supply Battalion
1st Tank Battalion	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Tank Battalion
22nd Marine Expeditionary Unit (MEU)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 22nd Marine Expeditionary Unit
23rd Marine Regiment	San Bruno, CA	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment
24th Marine Expeditionary Unit (MEU)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 24th Marine Expeditionary Unit
24th Marine Regiment	Kansas City, MO	CG 4th MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment
25th Marine Regiment	Fort Devens, MA	CG 4th MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment
26th Marine Expeditionary Unit (MEU)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 26th Marine Expeditionary Unit
2d Marine Special Operations Battalion	Camp Lejeune, NC	CG MARSOC	RNOSC-LANT	MITSC East	U.S. Marine Corps Forces, Special Operations Command > 2d Marine Special Operations Battalion
2nd Assault Amphibian Battalion (2nd AAV BN)	Camp Lejeune, NC	CO 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Assault Amphibian Battalion
2nd Battalion, 10th Marines (2/10)	Camp Lejeune, NC	CO 10th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 10th Marine Regiment > 2nd Battalion, 10th Marines
2nd Battalion, 11th Marines (2/11)	Camp Pendleton, CA	CO 11th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 11th Marine Regiment > 2nd Battalion, 11th Marines
2nd Battalion, 14th Marines (2/10)	Grand Prairie, TX	CO 14th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 2nd Battalion, 14th Marines
2nd Battalion, 1st Marines (2/1)	Camp Pendleton, CA	CO 1st Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Marine Regiment > 2nd Battalion, 1st Marines
2nd Battalion, 23rd Marines (2/23)	Pasadena, CA	CO 23rd Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 2nd Battalion, 23rd Marines
2nd Battalion, 24th Marines (2/24)	Chicago, IL	CO 24th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 2nd Battalion, 24th Marines
2nd Battalion, 25th Marines (2/25)	Garden City, NY	CO 25th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 2nd Battalion, 25th Marines

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
2nd Battalion, 2nd Marines (2/2)	Camp Lejeune, NC	CO 2d Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Marine Regiment > 2nd Battalion, 2nd Marines
2nd Battalion, 3rd Marines (2/3)	Kaneohe Bay, HI	CO 3d Marines	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 3rd Marine Regiment > 2nd Battalion, 3rd Marines
2nd Battalion, 4th Marines (2/4)	Camp Pendleton, CA	CO 5th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 5th Marine Regiment > 2nd Battalion, 4th Marines
2nd Battalion, 5th Marines (2/5)	Camp Pendleton, CA	CO 5th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 5th Marine Regiment > 2nd Battalion, 5th Marines
2nd Battalion, 6th Marines (2/6)	Camp Lejeune, NC	CO 6th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 6th Marine Regiment > 2nd Battalion, 6th Marines
2nd Battalion, 7th Marines (2/7)	29 Palms, CA	CO 7th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 7th Marine Regiment > 2nd Battalion, 7th Marines
2nd Battalion, 8th Marines (2/8)	Camp Lejeune, NC	CO 8th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 8th Marine Regiment > 2nd Battalion, 8th Marines
2nd Battalion, 9th Marines (2/9)	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Battalion, 9th Marines
2nd Combat Engineer Battalion (2nd CEB BN)	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Combat Engineer Battalion
2nd Dental Battalion	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > 2nd Dental Battalion
2nd Light Armored Recon Battalion	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Light Armored Recon Battalion
2nd Low Altitude Air Defense Battalion	Cherry Point, NC	CO MACG 28	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Air Control Group 28 > 2nd Low Altitude Air Defense
2nd Maintenance Battalion	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > 2nd Maintenance Battalion
2nd Marine Aircraft Wing (MAW)	Cherry Point, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing
2nd Marine Division (MARDIV)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division
2nd Marine Expeditionary Brigade (MEB)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Expeditionary Brigade
2nd Marine Logistics Group (FWD)	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > 2nd Marine Logistics Group (FWD)
2nd Marine Logistics Group (MLG)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group
2nd Marine Regiment	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Marine Regiment
2nd Medical Battalion	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > 2nd Medical Battalion
2nd Reconnaissance Battalion	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Reconnaissance Battalion
2nd Supply Battalion	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > 2nd Supply Battalion

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
2nd Tank Battalion	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Tank Battalion
31st Marine Expeditionary Unit (MEU)	Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 31st Marine Expeditionary Unit
3rd Air-Naval Gunfire Liaison Company (3rd ANGLICO)	Long Beach, CA	COMMARFORRES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 3rd Air-Naval Gunfire Liaison Company
3rd Assault Amphibian Battalion	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 3rd Assault Amphibian Battalion
3rd Battalion, 10th Marines (3/10)	Camp Lejeune, NC	CO 10th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 10th Marine Regiment > 3rd Battalion, 10th Marines
3rd Battalion, 14th Marines (3/14)	Philadelphia, PA	CO 14th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 3rd Battalion, 14th Marines
3rd Battalion, 1st Marines (3/1)	Camp Pendleton, CA	CO 1st Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Marine Regiment > 3rd Battalion, 1st Marines
3rd Battalion, 23rd Marines (3/23)	Belle Chase, LA	CO 23rd Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 3rd Battalion, 23rd Marines
3rd Battalion, 24th Marines (3/24)	Bridgeton, MO	CO 24th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 3rd Battalion, 24th Marines
3rd Battalion, 25th Marines (3/25)	Brook Park, OH	CO 25th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 3rd Battalion, 25th Marines
3rd Battalion, 2nd Marines (3/2)	Camp Lejeune, NC	CO 2d Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Marine Regiment > 3rd Battalion, 2nd Marines
3rd Battalion, 3rd Marines (3/3)	Kaneohe Bay, HI	CO 3d Marines	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 3rd Marine Regiment > 3rd Battalion, 3rd Marines
3rd Battalion, 4th Marines (3/4)	29 Palms, CA	CO 7th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 7th Marine Regiment > 3rd Battalion, 4th Marines
3rd Battalion, 5th Marines (3/5)	Camp Pendleton, CA	CO 5th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 5th Marine Regiment > 3rd Battalion, 5th Marines
3rd Battalion, 6th Marines (3/6)	Camp Lejeune, NC	CO 6th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 6th Marine Regiment > 3rd Battalion, 6th Marines
3rd Battalion, 7th Marines (3/7)	29 Palms, CA	CO 7th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 7th Marine Regiment > 3rd Battalion, 7th Marines
3rd Battalion, 8th Marines (3/8)	Camp Lejeune, NC	CO 8th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 8th Marine Regiment > 3rd Battalion, 8th Marines
3rd Battalion, 9th Marines (3/9)	Camp Lejeune, NC	CO 2d Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 2nd Marine Regiment > 3rd Battalion, 9th Marines
3rd Dental Battalion	Okinawa, Japan	CG 3d MLG	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Logistics Group > 3rd Dental Battalion
3rd Force Reconnaissance Battalion	Camp Schwab, Okinawa, Japan	CG 3 MARDIV	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 3rd Force Reconnaissance Battalion
3rd Force Reconnaissance Company (3rd FORECONCO)	Mobile, AL	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 3rd Force Reconnaissance Company
3rd Intelligence Battalion	Camp Hansen, Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Intelligence Battalion
3rd Light Armored Reconnaissance Battalion	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 3rd Light Armored Reconnaissance Battalion

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
3rd Low Altitude Air Defense Battalion	Camp Pendleton, CA	CO MACG-38	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38 > 3rd Low Altitude Air Defense Battalion
3rd Marine Aircraft Wing (MAW)	MCAS Miramar, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing
3rd Marine Division (MARDIV)	Camp Courtney, Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division
3rd Marine Expeditionary Brigade	Camp Courtney, Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Expeditionary Brigade
3rd Marine Logistics Group (MLG)	Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Logistics Group
3rd Marine Regiment	Kaneohe Bay, HI	CG 3 MARDIV	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 3rd Marine Regiment
3rd Platoon, A Company, 4th AAV BN	Gulfport, MS	CO A CO	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > A Company > 3rd Platoon
3rd Platoon, B Company, 4th AAV BN	Galveston, TX	CO B CO	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > B Company > 3rd Platoon
4th Air-Naval Gunfire Liaison Company (4th ANGLICO)	West Palm Beach, FL	COMMARFOR RES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Air-Naval Gunfire Liaison Company
4th Assault Amphibian (4th AAV) Battalion	Tampa, FL	CG MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion
4th Battalion, 14th Marines (4/14)	Bessemer, AL	CO 14th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 4th Battalion, 14th Marines
4th Civil Affairs Group (4th CAG)	Anacostia Annex, Washington, DC	COMMARFOR RES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Civil Affairs Group
4th Combat Engineer Battalion (CEB)	Baltimore, MD	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Combat Engineer Battalion
4th Dental Battalion	Marietta, GA	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Dental Battalion
4th Force Reconnaissance Company (4th FORECONCO)	Alameda, CA	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Force Reconnaissance Company
4th Landing Support Battalion	Fort Lewis, WA	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Landing Support Battalion
4th Light Armored Reconnaissance (LAR) Battalion	Camp Pendleton, CA	CG 4 MARDIV	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Division > 4th Light Armored Reconnaissance Battalion
4th Maintenance Battalion	Charlotte, NC	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Maintenance Battalion
4th Marine Aircraft Wing (MAW)	New Orleans, LA	COMMARFOR RES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing
4th Marine Corps District (MCD)	New Cumberland, PA	CG MCRC	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District
4th Marine Division (MARDIV)	New Orleans, LA	COMMARFOR RES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division
4th Marine Expeditionary Battalion (AT)	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 4th Marine Expeditionary Battalion (AT)
4th Marine Logistics Group (MLG)	New Orleans, LA	COMMARFOR RES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
4th Marine Logistics Group (MLG), G-3/5 .249	New Orleans, LA	COMMARFOR RES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group
4th Marine Regiment	Camp Schwab, Okinawa, Japan	CG 3 MARDIV	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 4th Marine Regiment
4th Medical Battalion	San Diego, CA	CG 4th MLG	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Logistics Group > 4th Medical Battalion
4th Reconnaissance Battalion	San Antonio, TX	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Reconnaissance Battalion
4th Supply Battalion	Newport News, VA	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Supply Battalion
4th Tank Battalion	San Diego, CA	CG 4 MARDIV	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Division > 4th Tank Battalion
5th Battalion (5/11)	Camp Pendleton, CA	CO 11th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 11th Marine Regiment > 5th Battalion (5/11)
5th Battalion, 10th Marines	Camp Lejeune, NC	CO 10th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 10th Marine Regiment > 5th Battalion, 10th Marines
5th Battalion, 14th Marines	Seal Beach, CA	CO 14th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 5th Battalion, 14th Marines
5th Marine Regiment	Camp Pendleton, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 5th Marine Regiment
6th Communications Battalion	Brooklyn, NY	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Communications Battalion
6th Engineer Support Battalion	Portland, OR	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Spt Bn
6th Marine Corps District (MCD)	Parris Island, SC	CG MCRC	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District
6th Marine Regiment	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 6th Marine Regiment
6th Motor Transport Battalion	Red Bank, NJ	CG 4th MLG	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Motor Transport Battalion
7th Communication Battalion	Camp Hansen, Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 7th Communication Battalion
7th Engineer Support Battalion	Camp Pendleton, CA	CG 1 MLG	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > 7th Engineer Support Battalion
7th Marine Regiment	29 Palms, CA	CG 1 MAR DIV	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 7th Marine Regiment
8th Engineer Support Battalion	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > 8th Engineer Support Battalion
8th Marine Corps District (MCD)	Fort Worth, TX	CG MCRC	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District
8th Marine Regiment	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 8th Marine Regiment
8th Tank Battalion	Rochester, NY	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 8th Tank Battalion
9th Engineer Support Battalion	Camp Butler, Okinawa, Japan	CG 3d MLG	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Logistics Group > 9th Engineer Support Battalion
9th Marine Corps District (MCD)	Kansas City, MO	CG MCRC	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District
9th Marine Expeditionary Brigade (MEB)	Camp Pendleton, CA	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 9th Marine Expeditionary Brigade
A Company, 1/24	Grand Rapids, MI	CO 1/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 1st Battalion > A Company
A Company, 1/25	Topsham, ME	CO 1/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 1st Battalion > A Company

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
A Company, 4th AAV BN	Little Creek, VA	CO 4th AAV BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > A Company
A Company, 4th CEB	Charleston, WV	CO 4th CEB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Combat Engineers Battalion > A Company
A Company, 4th TANK BN	Fort Knox, KY	CO 4th TANK BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Tank Battalion > A Company
Administration and Resource Division	Arlington, VA	DMCS	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Director Marine Corps Staff > Administration and Resource Division
ALD, 4th Marine Aircraft Wing (MAW)	New Orleans, LA	CG 4 MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > ALD
Alfred M Gray Marine Corps Research Center	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Alfred M Gray Marine Corps Research Center
Alternate Marine Corps Network Operations and Security Center (ALTNOSC)	Camp Pendleton, CA	MCNOSC	MCNOSC	MCNOSC	Marine Forces US Strategic Command > Marine Corps Network Operations and Security Center > Alternate Marine Corps Network Operations and Security Center
American Red Cross	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > American Red Cross
Ammunitions Company (AMMO Co), 4th SUP BN	Greenville, SC	CO 4th SUP BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Supply Battalion > Ammunitions Company
Anti-Tank Training Company (AT TOW Co.), 4th MARDIV	Broken Arrow, OK	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserves > 4th Marine Division > Anti-Tank Training Company
Anti-Terrorism Battalion (AT BN)	Bessemer, AL	CG 4 MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserves > 4th Marine Division > Anti-Terrorism Battalion
Assistant Commandant of the Marine Corps (ACMC)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Assistant Commandant of the Marine Corps
ATFP, Marine Corps Mobilization Command (MOBCOM)	Kansas City, MO	COMMARFORRES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > Marine Corps Mobilization Command
Aviation	Washington, DC	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Aviation
B Company, 1/23	Bossier City, LA	CO 1/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 1st Battalion > B Company
B Company, 1/24	Saginaw, MI	CO 1/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 1st Battalion > B Company
B Company, 1/25	Londonerry, NH	CO 1/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 1st Battalion > B Company
B Company, 4th AAV BN	Jacksonville, FL	CO 4th AAV BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > B Company
B Company, 4th CEB	Roanoke, V**A**	CO 4th CEB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Combat Engineers Battalion > B Company
B Company, 4th RECON BN	Billings, MT	CO 4th RECON BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Reconnaissance Battalion > B Company
B Company, 4th TANK BN	Yakima, WA	CO 4th TANK BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Tank Battalion > B Company
Beach and Terminal Operations Company A (BTO Co A)	San Jose, CA	CO 4th LSB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Landing Support Battalion > Beach and Terminal Operations Company A
Beach and Terminal Operations Company B (BTO Co B)	Savannah, GA	CO 4th LSB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Landing Support Battalion > Beach and Terminal Operations Company B

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Blount Island Command (BIC)	Jacksonville, NC	CG MARCORLOGCOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Logistics Command > Blount Island Command
Bridge Company B, 6th ESB	Folsom, PA	CO 6th ESB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Support Battalion > Bridge Company B
Bulk Fuel Company A, 6th ESB	Tucson, AZ	CO 6th ESB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Support Battalion > Bulk Fuel Company A
C Company, 1/23	Harlingen, TX	CO 1/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 1st Battalion > C Company
C Company, 1/24	Lansing, MI	CO 1/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 1st Battalion > C Company
C Company, 1/25	Plainville, CT	CO 1/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 1st Battalion >CB Company
C Company, 4th AAV BN	Lynchburg, TN	CO 4th AAV BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > C Company
C Company, Intelligence Support Battalion (INTELSPTBN)	Camp Upshur, Quantico, VA	CO INTELSPTBN	RNOSC-NCR	MITSC NCR	Marine Forces Reserve > Intelligence Support Battalion > C Company
Camp Mujuk	Camp Mujuk, Korea	COMMARFORK	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > Marine Forces Korea > Camp Mujuk
Center for Advanced Operational Culture Learning (CAOCL)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Center for Advanced Operational Culture Learning
Center for Irregular Warfare (CIW)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Center for Irregular Warfare
Chaplain of the Marine Corps	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Chaplain of the Marine Corps
Chemical Biological Incident Response Force (CBIRF)	Indian Head, MD	CG II MEF	RNOSC-NCR	MITSC NCR	Marine Forces Command > II Marine Expeditionary Force > Chemical Biological Incident Response Force (CBIRF)
College of Continuing Education	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > College of Continuing Education
Combat Assault Battalion	Camp Schwab, Okinawa, Japan	CG 3D MAR DIV	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > Combat Assault Battalion
Combat Logistics Battalion 7	29 Palms, CA	CG 1 MLG	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > Combat Logistics Battalion 7
Combat Logistics Regiment 1	Camp Pendleton, CA	CG 1 MLG	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > Combat Logistics Regiment 1
Combat Logistics Regiment 17	Camp Pendleton, CA	CG 1 MLG	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Logistics Group > Combat Logistics Regiment 17
Combat Logistics Regiment 3	Camp Foster, Okinawa, Japan	CG 3d MLG	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Logistics Group > Combat Logistics Regiment 3
Combat Logistics Regiment 35	Camp Kinser, Okinawa, Japan	CG 3d MLG	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Logistics Group > Combat Logistics Regiment 35
Combat Logistics Regiment 37	Camp Kinser, Okinawa, Japan	CG 3d MLG	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Logistics Group > Combat Logistics Regiment 37
Combat Service Support Detachment 21	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > Combat Service Support Detachment 21
Combat Service Support Detachment 23	Camp Lejeune, NC	CG 2nd MLG	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Logistics Group > Combat Service Support Detachment 23

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Combined Arms Training Center Camp Fuji	Camp Fuji, Japan	CG MCBJ	RNOSC-PAC	MITSC WestPac	Marine Corps Installations West > Marine Corps Bases Japan > Marine Corps Base Camp Butler > Combined Arms Training Center Camp Fuji
Command, Control, Communications and Computers (C4)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Command, Control, Communications and Computers
Commandant of the Marine Corps (CMC)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Commandant of the Marine Corps
Communications Company (Comm Co), H&S BN	Greensboro, NC	CO H&S BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Communications Company
Communications Company (Comm Co), HQBN	Cincinnati, OH	CO HQBN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > Headquarters Battalion > Communications Company
Communications School	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Communications School
Company C (Rein), 4th Landing Support Co., 4th MLG, 4th LSB	Charleston, SC	CO 4th LS Co	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Landing Support Battalion > Landing Support Equipment Company > Company C (Rein)
Counsel for the Commandant	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Counsel for the Commandant
D Battery, 2/14	El Paso, TX	CO 2/14	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 2nd Battalion > D Battery
D Company, 4th AAV BN	Knoxville, TN	CO 4th AAV BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > D Company
D Company (D Co), 4th RECON BN	Albuquerque, NM	CO 4th RECONBN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Reconnaissance Battalion > D Company
D Company, 4th TANK BN	Riverside, CA	CO 4th TANK BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Tank Battalion > D Company
Defense Commissary Agency	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Defense Commissary Agency
Defense Language Institute (DLI)	Monterey, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Defense Language Institute
Detachment, 4th FORECONCO	MCB Kaneohe Bay, HI	CG 4 MARDIV	RNOSC-PAC	MITSC MidPac	Marine Forces Reserve > 4th Marine Division > 4th Force Reconnaissance Company > Detachment
Detachment, Comm Co, HQBN	Indianapolis, IN	CO HQBN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > Headquarters Battalion > Communications Company > Detachment
Detachment, HQSVCCO, 4th MED BN	Orlando, FL	CO HQSVCCO	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Medical Battalion > Headquarters and Service Company, Detachment
Detachment , MP Co, HQBN	Wahpeton, ND	CO MP Co	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > Headquarters Battalion > Military Police Company > Detachment
Detachment 1, BTO Co A	Wilmington, NC	CO BTO Co A	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Landing Support Battalion > Beach and Terminal Operations Company A > Detachment 1
Detachment 1, Bulk Fuel Company B, 6th ESB	Green Bay, WI	CO Bulk Fuel Co B	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Support Battalion > Bulk Fuel Company B > Detachment 1
Detachment 1, Comm Co, H&S BN	Grissom ARB, Peru, IN	CO CommCo	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Communications Company Detachment 1
Detachment 1 Engineers, Electronic Maintenance Company (ELMACO)	Wichita, KA	CO ELMACO	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Maintenance Battalion > Electronic Maintenance Company > Detachment 1, Engineers

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Detachment 1, H&S Co, 8th TANK BN	Hialeah, FL	CO H&S Co	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 8th Tank Battalion > Headquarters and Service Company > Detachment 1
Detachment 2, AMMO Co, 4th SUP BN	Topeka, KS	CO AMMO Co	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Supply Battalion > Ammunitions Company > Detachment 2
Detachment 2, BTO Co A	Concord, CA	CO BTO Co A	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Landing Support Battalion > Beach and Terminal Operations Company A > Detachment 2
Detachment 2, Comm Co, H&S BN	Allentown, PA	CO CommCo	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Communications Company Detachment 2
Detachment A, MAG-49	Marietta, GA	CO MAG-49	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49, Detachment A
Detachment B, HMLA 773	Johnstown, PA	CO HMLA 773	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 42, Marine Light Attack Helicopter Squadron 773, Detachment B
Detachment B, MAG-46	Edwards AFB, CA	CO MAG-46	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 46, Detachment B
Detachment C, MAG-49	NAS Belle Chase, LA	CO MAG-49	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49, Detachment C
Detachment D, MAG-49	NAS Norfolk, VA	CO MAG-49	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49, Detachment D
Director Marine Corps Staff	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Director Marine Corps Staff
Division of Public Affairs	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Division of Public Affairs
E Company, 2/24	Des Moines, IA	CO 2/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 2nd Battalion > E Company
E Company, 2/25	Harrisburg, PA	CO 2/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 2nd Battalion > E Company
E Company, 4th AAV BN	Syracuse, NY	CO 4th AAV BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 4th Assault Amphibian Battalion > E Company
Engineer Company A (ENGR CO A), 6th ESB	Eugene, OR	CO 6th ESB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Support Battalion > Engineer Company A
Engineer Company B (ENGR CO B), 6th ESB	South Bend, IN	CO 6th ESB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Support Battalion > Engineer Company B
Engineer School	Camp Lejeune, NC	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Engineer School
Engineer Support Company (ENGSPT Co), 6th ESB	Battle Creek, MI	CO 6th ESB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Engineer Support Battalion > Engineer Support Company
Enlisted PME	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Enlisted PME
Enterprise Service Desk (ESD)	Kansas City, MO	MCNOSC	MCNOSC	MCNOSC	Marine Forces US Strategic Command > Marine Corps Network Operations and Security Center > Enterprise Service Desk
Expeditionary Force Development Center (EFDC)	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Expeditionary Force Development Center
Expeditionary Warfare School	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Expeditionary Warfare School
Expeditionary Warfare Training Group, Atlantic (EWTGLANT)	Norfolk, VA	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Expeditionary Warfare Training Group, Atlantic (EWTGLANT)
Expeditionary Warfare Training Group, Pacific (EWTGPAC)	San Diego, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Expeditionary Warfare Training Group, Pacific (EWTGPAC)
F Battery, 2/14	Oklahoma City, OK	CO 2/14	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 2nd Battalion > F Battery
F Company, 2/23	Salt Lake City, UT	CO 2/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 2nd Battalion > F Company

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
F Company, 2/24	Milwaukee, WI	CO 2/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 2nd Battalion > F Company
F Company, 2/25	Albany, NY	CO 2/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 2nd Battalion > F Company
Field Medical Training Battalion-East	Camp Lejeune, NC	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Field Medical Training Battalion-East
Field Medical Training Battalion-West	Camp Pendleton, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Field Medical Training Battalion-West
G Company, 2/23	Los Alamitos, CA	CO 2/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 2nd Battalion > G Company
G Company, 2/24	Madison, WI	CO 2/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 2nd Battalion > G Company
G Company, 2/25	Dover, NJ	CO 2/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 2nd Battalion > G Company
Headquarters and Service Battalion (H&S BN)	Marietta, GA	CG 4th MLG	RNOSC-RES	MITSC Reseres	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion
Headquarters Company (HQ Co.), H&S BN	Marietta, GA	CO H&S BN	RNOSC-RES	MITSC Reseres	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Headquarters Company
Headquarters and Service Battalion	Belton, MO	CO 24th Marines	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 2nd Battalion, 24th Marines > Headquarters and Service Battalion
Headquarters Battalion, 2nd Marine Division	Camp Lejeune, NC	CG 2 MARDIV	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > Headquarters Battalion, 2nd Marine Division
Headquarters Marine Corps (HQMC)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps
Health Services	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Health Services
HQ MFP, Camp Smith	Camp Smith, Hawaii	MARCORBASESPAC	RNOSC-PAC	MITSC MidPac	MARCORBASESPAC > Marine Corps Base Hawaii, Camp Smith
HQMC Headquarters Battalion	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > HQMC Headquarters Battalion
Human Resources and Organizational Management	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Human Resources and Organizational Management
I Company, 3/24	Nashville, TN	CO 3/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 3rd Battalion > I Company
I Company, 3/23	North Little Rock, AR	CO 3/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 3rd Battalion > I Company
I Marine Expeditionary Force (MEF)	Camp Pendleton, CA	COMMARFORPAC	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force
I MEF Augmentation Command Element (I MACE)	Camp Pendleton, CA	COMMARFORRES	RNOSC-PAC	MITSC West	Marine Forces Reserve > I MEF Augmentation Command Element
II Marine Expeditionary Force	Camp Lejeune, NC	COMMARFORCOM	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force
II Marine Expeditionary Forces Forward	Al Asad, Iraq	CG MNF-W		Self	Marine Forces Command > II Marine Expeditionary Force Forward
II MEF Headquarters Group	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > II MEF Headquarters Group
III Marine Expeditionary Force	Camp Courtney, Okinawa, Japan	COMMARFORPAC	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force *(CG III MEF also serves as CG Marine Corps Bases Japan)*
III MEF Headquarters Group	Camp Courtney,	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > III MEF Headquarters Group

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
	Okinawa, Japan				
Inspector General of the Marine Corps	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Inspector General of the Marine Corps
Installations & Logistics (I&L)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Installations & Logistics
Intelligence	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Intelligence
Intelligence Training and Education Center of Excellence	Dam Neck, VA	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Intelligence Training and Education Center of Excellence
Iraq Investigations	Tampa, FL	MARFORCENT	RNOSC-LANT	MITSC East	Marine Forces Central > Iraq Investigations
Joint Non Lethal Weapons Directorate (JNLWD)	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Joint Non Lethal Weapons Directorate
K Battery, 2/14	Huntsville, AL	CO 2/14	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 2nd Battalion > K Battery
K Company, 3/24	Terre Haute, IN	CO 3/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 3rd Battalion > K Company
K Company, 3/25	Moundsville, WV	CO 3/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 3rd Battalion > K Company
L Company, 3/23	Montgomery, AL	CO 3/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 3rd Battalion > L Company
L Company, 3/24	Johnson City, TN	CO 3/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 3rd Battalion > L Company
L Company, 3/25	Columbus, OH	CO 3/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 3rd Battalion > L Company
Landing Support Equipment Company (LSPT EQUIP Co), 4th LSB	Vienna, OH	CO 4th LSB	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 6th Landing Support Battalion > Landing Support Equipment Company
Los Angeles Public Affairs	Los Angeles, CA	Dir, Public Affairs	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Division of Public Affairs > Branches > Los Angeles Public Affairs
M Battery, 3/14	Chattanooga, TN	CO 3/14	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 14th Marine Regiment > 3rd Battalion > M Battery
Maintenance Center Albany	Albany, GA	CG MARCORLOGCOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Maintenance Center Albany
Maintenance Center Barstow	Barstow, CA	CGMARCORLOGCOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Maintenance Center Barstow
Manpower & Reserve Affairs	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Manpower & Reserve Affairs
Marine Aerial Refueler Transport Squadron 152	MCAS Futenma, Okinawa, Japan	CO MAG-36	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 36 > Marine Aerial Refueler Transport Squadron
Marine Aerial Refueler Transport Squadron 234 (VMGR-234)	Fort Worth, TX	CO MAG-41	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 41 > Marine Aerial Refueler Transport Squadron 234
Marine Aerial Refueler Transport Squadron 252	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Aerial Refueler Transport
Marine Aerial Refueler Transport Squadron 352	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Aerial Refueler Transport Squadron 352
Marine Aerial Refueler Transport Squadron 452 (VMGR-452)	Newburgh, NY	CO MAG-49	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49 > Marine Aerial Refueler Transport Squadron 452

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Air Control Group 18	MCAS Futenma, Okinawa, Japan	CG 1st MAW	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18
Marine Air Control Group 28	Cherry Point, NC	CG 2d MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Air Control Group 28
Marine Air Control Group 38	MCAS Miramar, CA	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38
Marine Air Control Group 48	Great Lakes, IL	CG 4th MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Air Control Group 48
Marine Air Control Group 48 Headquarters	Great Lakes, IL	CG 4th MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Air Control Group 48 Headquarters
Marine Air Control Squadron 1	Yuma, AZ	CO MACG-38	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38 > Marine Air Control Squadron 1
Marine Air Control Squadron 2	MCAS Cherry Point, NC	CO MACG-18	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18 > Marine Air Support Squadron 2
Marine Air Control Squadron 23	Aurora, CO	CO MACG-48	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Air Control Group 48 > Marine Air Control Squadron 23
Marine Air Control Squadron 24	Dam Neck, VA	CO MACG-48	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Air Control Group 48 > Marine Air Control Squadron 24
Marine Air Control Squadron 4	MCAS Futenma, Okinawa, Japan	CO MACG-18	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18 > Marine Air Control Squadron 4
Marine Air Support Squadron 1	Cherry Point, NC	CO MACG 28	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Air Control Group 28 > Marine Air Support Squadron 1
Marine Air Support Squadron 2	MCAS Futenma, Okinawa, Japan	CO MACG-18	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18 > Marine Air Support Squadron 2
Marine Air Support Squadron 3	Camp Pendleton, CA	CO MACG-38	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38 > Marine Air Support Squadron 3
Marine Air Support Squadron 6 (MASS-6)	Chicopee, MA	CO MACG-48	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Air Control Group 48 > Marine Air Support Squadron 6
Marine Aircraft Group 11	MCAS Miramar, CA	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11
Marine Aircraft Group 12	Iwakuni, Japan	CG 1st MAW	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 12
Marine Aircraft Group 13	Yuma, AZ	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 13
Marine Aircraft Group 14	Cherry Point, NC	CG 2d MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14
Marine Aircraft Group 16	MCAS Miramar, CA	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16
Marine Aircraft Group 24	Kaneohe Bay, HI	CG 1st MAW	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 24
Marine Aircraft Group 26	New River, NC	CG 2d MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26
Marine Aircraft Group 29	New River, NC	CG 2d MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
					Group 29
Marine Aircraft Group 31	Beaufort, SC	CG 2d MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31
Marine Aircraft Group 36	Futenma, Japan	CG 1st MAW	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 36
Marine Aircraft Group 39	Camp Pendleton, CA	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39
Marine Aircraft Group 41	Fort Worth, TX	CG 4 MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 41
Marine Aircraft Group 42	Marietta, GA	CG 4th MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 42
Marine Aircraft Group 46	Miramar, CA	CG 4th MAW	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 46
Marine Aircraft Group 49	Willow Grove, PA	CG 4th MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49
Marine All Weather Fighter Attack Squadron 242	Iwakuni, Japan	CO MAG-12	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 12 > Marine All Weather Fighter Attack
Marine Attack Squadron 211	Yuma, AZ	CO MAG-13	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 13 > Marine Attack Squadron 211
Marine Attack Squadron 214	Yuma, AZ	CO MAG-13	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 13 > Marine Attack Squadron 214
Marine Attack Squadron 223	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Attack Squadron 223
Marine Attack Squadron 231	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Attack Squadron 231
Marine Attack Squadron 311	Yuma, AZ	CO MAG-13	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 13 > Marine Attack Squadron 311
Marine Attack Squadron 513	Yuma, AZ	CO MAG-13	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 13 > Marine Attack Squadron 513
Marine Attack Squadron 542	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Attack Squadron 542
Marine Attack Training Squadron 203	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Attack Training Squadron 203
Marine Aviation Detachment China Lake	China Lake, CA	DepCmdnt for Aviation	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Aviation > Marine Aviation Detachment China Lake
Marine Aviation Logistics Squadron 11	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Aviation Logistics Squadron 11
Marine Aviation Logistics Squadron 12	Iwakuni, Japan	CO MAG-12	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 12 > Marine Aviation Logistics Squadron 12
Marine Aviation Logistics Squadron 13	Yuma, AZ	CO MAG-13	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 13 > Marine Aviation Logistics Squadron 13
Marine Aviation Logistics Squadron 14	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Aviation Logistics Squadron 14
Marine Aviation Logistics Squadron 16	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Aviation Logistics Squadron 16

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Aviation Logistics Squadron 24	Kaneohe Bay, HI	CO MAG-24	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 24 > Marine Aviation Logistics Squadron 24
Marine Aviation Logistics Squadron 26	New River, NC	CO MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Aviation Logistics Squadron 26
Marine Aviation Logistics Squadron 29	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Aviation Logistics Squadron 29
Marine Aviation Logistics Squadron 31	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Aviation Logistics Squadron 31
Marine Aviation Logistics Squadron 36	MCAS Futenma, Okinawa, Japan	CO MAG-36	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 36 > Marine Aviation Logistics Squadron 36
Marine Aviation Logistics Squadron 39	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Aviation Logistics Squadron 39
Marine Aviation Logistics Squadron 41	Fort Worth, TX	CO MAG-41	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 41 > Marine Aviation Logistics Squadron 41
Marine Aviation Logistics Squadron 42	Marietta, GA	CO MAG-42	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 42 > Marine Aviation Logistics Squadron 42
Marine Aviation Logistics Squadron 46	San Diego, CA	CO MAG-46	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 46 > Marine Aviation Logistics Squadron 46
Marine Aviation Logistics Squadron 49	Newburgh, NY	CO MAG-49	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49 > Marine Aviation Logistics Squadron 49
Marine Aviation Training Support Group-21	NAS Pensacola, FL	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Marine Aviation Training Support Group-21
Marine Aviation Training Support Group-23	NAS Lemoore, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Marine Aviation Training Support Group-23
Marine Aviation Training Support Group-33	NAS Oceana, Virginia Beach, VA	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Marine Aviation Training Support Group-33
Marine Aviation Training Support Squadron-1	NAS Meridian, MS	CG TECOM	RNOSC-RES	MITSC Reserves	Headquarters Marine Corps > Training & Education Command > Marine Aviation Training Support Squadron-1
Marine Aviation Weapons and Tactics Squadron 1	Yuma, AZ	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aviation Weapons and Tactics Squadron 1
Marine Aviation Weapons and Tactics Squadron One	Yuma, AZ	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Marine Aviation Weapons and Tactics Squadron One
Marine Aviation Weapons and Tactics Squadron One (MAWTS-1)	Yuma, AZ	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Marine Aviation Weapons and Tactics Squadron One
Marine Barracks 8th & I	Washington, DC	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Marine Barracks 8th & I
Marine Corps Air Facility Quantico	Quantico, VA	CG MCI-East	RNOSC-NCR	MITSC NCR	Marine Corps Installations East > Marine Corps Air Facility Quantico
Marine Corps Air Ground Combat Center Twentynine Palms	29 Palms, CA	CG MCI-West	RNOSC-PAC	MITSC West	Marine Corps Installations West > Marine Corps Air Ground Combat Center Twentynine Palms
Marine Corps Air Station Beaufort	Beaufort, SC	CG MCI-East	RNOSC-LANT	MITSC East	Marine Corps Installations East > Marine Corps Air Station Beaufort

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Corps Air Station Camp Pendleton	Camp Pendleton, CA	CG MCI-West	RNOSC-PAC	MITSC West	Marine Corps Installations West > Marine Corps Air Station Camp Pendleton
Marine Corps Air Station Cherry Point	Cherry Point, NC	CG MCI-East	RNOSC-LANT	MITSC East	Marine Corps Installations East > Marine Corps Air Station Cherry Point
Marine Corps Air Station Futenma	Futenma, Japan	CG MCBJ	RNOSC-PAC	MITSC WestPac	Marine Corps Installations West > Marine Corps Bases Japan > Marine Corps Air Station Futenma
Marine Corps Air Station Iwakuni	Iwakuni, Japan	CG MCBJ	RNOSC-PAC	MITSC WestPac	Marine Corps Installations West > Marine Corps Bases Japan > Marine Corps Air Station Iwakuni
Marine Corps Air Station Miramar	MCAS Miramar, CA	CG MCI-West	RNOSC-PAC	MITSC West	Marine Corps Installations West > Marine Corps Air Station Miramar
Marine Corps Air Station New River	New River	CG MCI-East	RNOSC-LANT	MITSC East	Marine Corps Installations East > Marine Corps Air Station New River
Marine Corps Air Station Yuma	Yuma, AZ	CG MCI-West	RNOSC-PAC	MITSC West	Marine Corps Installations West > Marine Corps Air Station Yuma
Marine Corps Base Camp Butler	Camp Butler, Japan	CG MCBJ	RNOSC-PAC	MITSC WestPac	Marine Corps Installations West > Marine Corps Bases Japan > Marine Corps Base Camp Butler
Marine Corps Base Camp Lejeune	Camp Lejeune, NC	CG MCI-East	RNOSC-LANT	MITSC East	Marine Corps Installations East > Marine Corps Base Camp Lejeune
Marine Corps Base Camp Mujuk	Pohang, Korea	COMMARFORPAC	RNOSC-PAC	MITSC WetPac	Marine Corps Installations West > Marine Corps Base Camp Mujuk
Marine Corps Base Camp Pendleton	Camp Pendleton, CA	CG MCI-West	RNOSC-PAC	MITSC West	Marine Corps Installations West > Marine Corps Base Camp Pendleton
Marine Corps Base Hawaii	Kaneohe, Hawaii	MARCORBASESPAC	RNOSC-PAC	MITSC MidPac	Marine Corps Installations West > Marine Corps Base Hawaii
Marine Corps Base Pacific	Camp Smith, Hawaii	CMC	RNOSC-PAC		MARCORBASESPAC
Marine Corps Base Quantico	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico
Marine Corps Bases Japan	Japan	MARFORBASESPAC	RNOSC-PAC	MITSC WestPac	Marine Corps Installations West > Marine Corps Bases Japan *(CG Marine Corps Bases Japan also serves as CG III MEF)*
Marine Corps Combat Development Command (MCCDC)	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Combat Development Command *(CG MCCDC also serves as Dep Commandant for CD&I HQMC; CG MCINCR; and COMMARFORSTRAT)*
Marine Corps Combat Services Support School (MCCSSS)	Camp Lejeune, NC	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Marine Corps Combat Services Support School
Marine Corps Communication-Electronics School (MCCES)	29 Palms, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Marine Corps Communication-Electronics School
Marine Corps Community Services (MCCS)	Quantico, VA	Dir, M&RA	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Manpower & Reserve Affairs > Personal and Family Readiness Division > Marine Corps Community Services
Marine Corps Detachment Goodfellow AFB	Goodfellow AFB, TX	CG TECOM	RNOSC-RES	MITSC Reserves	Headquarters Marine Corps > Training & Education Command > Marine Corps Detachment Goodfellow AFB
Marine Corps Doctrine Division (MCDD)	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Doctrine Division
Marine Corps Embassy Security Group	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Combat Development Command > Marine Corps Embassy Security Group
Marine Corps Engineer Center of	Camp Lejeune, NC	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Marine Corps Engineer Center of Excellence

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Excellence (MCECOE)					(MCECOE)
Marine Corps Engineer School	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Marine Corps Engineer School
Marine Corps Installations East (MCI-East)	Camp Lejeune, NC	COMMARFORCOM	RNOSC-LANT	MITSC East	Marine Corps Installations East
Marine Corps Installations West	Camp Pendleton, CA	MARCORBASESPAC	RNOSC-PAC	MITSC West	MARCORBASESPAC > Marine Corps Installations West
Marine Corps Intelligence Activity (MCIA)	Quantico, VA	Dir, Intelligence	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Intelligence > Marine Corps Intelligence Activity
Marine Corps Intelligence School (MCIS)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Marine Corps Intelligence School
Marine Corps Logistics Base (MCLB) Barstow	Barstow, CA	CG MCI-West	RNOSC-PAC	MITSC West	Marine Corps Installations West > Marine Corps Logistics Base Barstow
Marine Corps Logistics Base Albany	Albany, GA	CG MCI-East	RNOSC-LANT	MITSC East	Marine Corps Installations East > Marine Corps Logistics Base Albany
Marine Corps Logistics Command (MARCORLOGCOM)	Albany, GA	HQMC I&L	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Logistics Command
Marine Corps Mobilization Command (MOBCOM),	Kansas City, MO	COMMARFORRES	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > Marine Corps Mobilization Command
Marine Corps Network Operations and Security Center (MCNOSC)	Quantico, VA	HQMC Director C4	MCNOSC	MCNOSC	Marine Forces US Strategic Command > Marine Corps Network Operations and Security Center
Marine Corps Recruit Depot Parris Island (MCRDPI)	Parris Island, SC	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > Marine Corps Recruit Depot Parris Island
Marine Corps Recruit Depot San Diego (MCRDSD)	San Diego, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Marine Corps Recruit Depot San Diego
Marine Corps Recruiting Command (MCRC)	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Recruiting Command
Marine Corps Security Force Regiment	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > Marine Corps Security Force Regiment
Marine Corps Studies System (MCSS)	Quantico, VA	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Studies System
Marine Corps Systems Command (MCSC)	Quantico, VA	ACMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Systems Command
Marine Corps Tactical Systems Support Activity (MCTSSA)	Quantico, VA	CG MCSC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Systems Command > Marine Corps Tactical Systems Support Activity
Marine Corps University (MCU)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Marine Corps University
Marine Corps Warfighting Lab (MCWL)	Quantico, VA	DC CD&I	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Warfighting Lab
Marine Cryptologic Support Battalion (MCSB)	Ft Meade, MD	CO MCIA	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Intelligence > Marine Corps Intelligence Activity > Marine Cryptologic Support Battalion
Marine Fighter Attack Squadron (All Weather)-332	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Fighter Attack Squadron (All Weather)-332

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Fighter Attack Squadron (All Weather)-533	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Fighter Attack Squadron (All Weather)-533
Marine Fighter Attack Squadron 112	Fort Worth, TX	CO MAG-41	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 41 > Marine Fighter Attack Squadron 112
Marine Fighter Attack Squadron 115	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Fighter Attack Squadron 115
Marine Fighter Attack Squadron 121	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Squadron 121
Marine Fighter Attack Squadron 122	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Fighter Attack Squadron 122
Marine Fighter Attack Squadron 142	Marietta, GA	CO MALS-42	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 42 > Marine Fighter Attack Squadron 142
Marine Fighter Attack Squadron 212	MCAS Iwakuni, Japan	CO MAG-12	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 12 > Marine Fighter Attack Squadron 212
Marine Fighter Attack Squadron 225	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Squadron 225
Marine Fighter Attack Squadron 232	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Squadron 232
Marine Fighter Attack Squadron 242	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Squadron 242
Marine Fighter Attack Squadron 251	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Fighter Attack Squadron 251
Marine Fighter Attack Squadron 312	Beaufort, SC	CO MAG 31	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 31 > Marine Fighter Attack Squadron 312
Marine Fighter Attack Squadron 314	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Squadron 314
Marine Fighter Attack Squadron 323	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Squadron 323
Marine Fighter Attack Training Squadron 101	MCAS Miramar, CA	CO MAG-11	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 11 > Marine Fighter Attack Training Squadron
Marine Fighter Attack Training Squadron 401	MCAS Miramar, CA	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Fighter Attack Training Squadron 401
Marine Fighter Training Squadron 401	Yuma, AZ	CO MAG-46	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 46 > Marine Fighter Training Squadron 401
Marine Forces Africa (MarForAfr)	Stuttgart, Germany	CMC & Cmdr USAFCOM	RNOSC-LANT	MITSC Europe	Marine Forces Africa
Marine Forces Central (MarForCent)	Tampa, FL	CMC & Cmdr USCENTCOM	RNOSC-LANT	MITSC East	Marine Forces Central
Marine Forces Command	Norfolk, VA	CMC & JFCOM/CC	RNOSC-LANT	MITSC East	Marine Forces Command *(COMMARFORCOM also serves as COMMARCORBASESLANT AND CG FMFLant)*
Marine Forces Cyber (MarForCyber)	Ft Meade, MD	CMC & Cmdr USCYBERCOM	RNOSC-NCR	MITSC NCR	Marine Forces US Cyber Command

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Forces Europe (MarForEur)	Stuttgart, Germany	CMC & Cmdr USEUCOM	RNOSC-LANT	MITSC Europe	Marine Forces Europe
Marine Forces Korea (MarForK)	Korea	COMMARFORPAC	RNOSC-PAC	MITSC WestPac	Marine Forces Korea
Marine Forces North (MarForNorth)	New Orleans, LA	CMC & Cmdr USNORTHCOM	RNOSC-RES	MITSC Reserves	Marine Forces North
Marine Forces Pacific (MarForPac)	Camp Smith, Hawaii	CMC & Cmdr USPACOM	RNOSC-PAC	MITSC West	Marine Forces Pacific *(COMMARFORPAC also serves as COMMARCORBASESPAC and CG FMFPAC)*
Marine Forces Reserve (MarForRes)	New Orleans, LA	CMC	RNOSC-RES	MITSC Reserves	Marine Forces Reserve
Marine Forces South (MarForSouth)	Miami, FL	CMC & Cmdr USSOUTHCOM	RNOSC-LANT	MITSC East	Marine Forces South (MarForSouth)
Marine Forces US Strategic Command (MarForStrat)	Omaha, NE	CMC & USSTRATCOM	RNOSC-RES	MITSC Reserves	Marine Forces US Strategic Command
Marine Heavy Helicopter Squadron 361	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Heavy Helicopter Squadron 361
Marine Heavy Helicopter Squadron 362	Japan	CO MAG-24	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 24 > Marine Heavy Helicopter Squadron 362
Marine Heavy Helicopter Squadron 363	Kaneohe Bay, HI	CO MAG-24	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 24 > Marine Heavy Helicopter Squadron 363
Marine Heavy Helicopter Squadron 461	New River, NC	Cmdr MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Heavy Helicopter Squadron 461
Marine Heavy Helicopter Squadron 462	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Heavy Helicopter Squadron 462
Marine Heavy Helicopter Squadron 463	Kaneohe Bay, HI	CO MAG-24	RNOSC-PAC	MITSC MidPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 24 > Marine Heavy Helicopter Squadron 463
Marine Heavy Helicopter Squadron 464	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Heavy Helicopter Squadron 464
Marine Heavy Helicopter Squadron 465	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Heavy Helicopter Squadron 465
Marine Heavy Helicopter Squadron 466	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Heavy Helicopter Squadron 466
Marine Heavy Helicopter Squadron 769	Edwards AFB, CA	CO MAG-46	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 46 > Marine Heavy Helicopter Squadron 769
Marine Heavy Helicopter Squadron 772	Willow Grove, PA	CO MAG-49	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 49 > Marine Heavy Helicopter Squadron 772
Marine Helicopter Squadron 1 (HMX-1)	Quantico, VA	CG II MEF	RNOSC-NCR	MITSC NCR	Marine Forces Command > II Marine Expeditionary Force > Marine Helicopter Squadron 1
Marine Helicopter Training Squadron 302	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Helicopter Training Squadron
Marine Helicopter Training Squadron 303	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Helicopter Training Squadron 303

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Light Attack Helicopter Squadron 167	New River, NC	CO MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Light Attack Helicopter
Marine Light Attack Helicopter Squadron 169	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Light Attack Helicopter Squadron 169
Marine Light Attack Helicopter Squadron 267	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Light Attack Helicopter Squadron 267
Marine Light Attack Helicopter Squadron 269	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Light Attack Helicopter Squadron 269
Marine Light Attack Helicopter Squadron 367	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Light Attack Helicopter Squadron 367
Marine Light Attack Helicopter Squadron 369	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Light Attack Helicopter Squadron 369
Marine Light Attack Helicopter Squadron 773	Marietta, GA	CO MALS-42	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 42 > Marine Light Attack Helicopter Squadron 773
Marine Light Attack Helicopter Squadron 775	Camp Pendleton, CA	CO MAG-46	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 46 > Marine Light Attack Helicopter Squadron 775
Marine Medium Helicopter Squadron 161	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Medium Helicopter Squadron 161
Marine Medium Helicopter Squadron 162	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Medium Helicopter Squadron 162
Marine Medium Helicopter Squadron 163	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Medium Helicopter Squadron 163
Marine Medium Helicopter Squadron 165	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Medium Helicopter Squadron 165
Marine Medium Helicopter Squadron 166	MCAS Miramar, CA	CO MAG-16	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 16 > Marine Medium Helicopter Squadron 166
Marine Medium Helicopter Squadron 261	New River, NC	CO MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Medium Helicopter Squadron 261
Marine Medium Helicopter Squadron 262	Japan	CO MAG-36	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 36 > Marine Medium Helicopter Squadron 262
Marine Medium Helicopter Squadron 263	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Medium Helicopter Squadron 263
Marine Medium Helicopter Squadron 264	New River, NC	CO MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Medium Helicopter Squadron 264
Marine Medium Helicopter Squadron 265	Okinawa, Japan	CO MAG-36	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Aircraft Group 36 > Marine Medium Helicopter Squadron 265
Marine Medium Helicopter Squadron 266	New River, NC	CO MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Medium Helicopter Squadron 266
Marine Medium Helicopter Squadron 268	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Medium Helicopter Squadron 268
Marine Medium Helicopter Squadron 364	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Medium Helicopter Squadron 364

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Medium Helicopter Squadron 365	New River, NC	CO MAG 29	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 29 > Marine Medium Helicopter Squadron 365
Marine Medium Helicopter Squadron 774	Marietta, GA	CO MALS-42	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Aircraft Group 42 > Marine Medium Helicopter Squadron 774
Marine Medium Helicopter Training Squadron 164	Camp Pendleton, CA	CO MAG-39	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Aircraft Group 39 > Marine Medium Helicopter Training Squadron 164
Marine Security Guard	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Marine Security Guard
Marine Special Operations Advisor Group	Camp Lejeune, NC	CG MARSOC	RNOSC-LANT	MITSC East	U.S. Marine Corps Forces, Special Operations Command > Marine Special Operations Advisor Group
Marine Special Operations School	Camp Lejeune, NC	CG MARSOC	RNOSC-LANT	MITSC East	U.S. Marine Corps Forces, Special Operations Command > Marine Special Operations School
Marine Special Operations Support Group	Camp Lejeune, NC	CG MARSOC	RNOSC-LANT	MITSC East	U.S. Marine Corps Forces, Special Operations Command > Marine Special Operations Support Group
Marine Tactical Air Command Squadron 18	Okinawa, Japan	CO MACG-18	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18 > Marine Tactical Air Command Squadron 18
Marine Tactical Air Command Squadron 28	Cherry Point, NC	CO MACG 28	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Air Control Group 28 > Marine Wing Communications Squadron 28
Marine Tactical Air Command Squadron 38	MCAS Miramar, CA	CO MACG-38	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38 > Marine Tactical Air Command Squadron 38
Marine Tactical Air Command Squadron 48 (MTACS-48)	Great Lakes, IL	CO MACG-48	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Air Control Group 48 > Marine Tactical Air Command Squadron 48
Marine Tactical Electronic Warfare Squadron-1	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Tactical Electronic Warfare Squadron-1
Marine Tactical Electronic Warfare Squadron-2	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Tactical Electronic Warfare Squadron-2
Marine Tactical Electronic Warfare Squadron-3	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Tactical Electronic Warfare Squadron-3
Marine Tactical Electronic Warfare Squadron-4	Cherry Point, NC	CO MAG 14	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 14 > Marine Tactical Electronic Warfare Squadron-4
Marine Tiltrotor Training Squadron 204	New River, NC	CO MAG 26	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Aircraft Group 26 > Marine Tiltrotor Training Squadron 204
Marine Transport Squadron (VMR), Detachment	Andrews AFB, MD	CO VMR	RNOSC-RES	MITSC Reserves	Marine Forces Reserves > 4th Marine Air Wing > Marine Transport Squadron > Detachment
Marine Unmanned Aerial Vehicle Squadron 1	29 Palms, CA	CO MACG-38	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38 > Marine Unmanned Aerial Vehicle Squadron 1
Marine Unmanned Aerial Vehicle Squadron-2	Cherry Point, NC	CO MACG 28	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Air Control Group 28 > Marine Unmanned Aerial Vehicle Squadron-2
Marine Wing Communications Squadron 18	Okinawa, Japan	CO MACG-18	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Air Control Group 18 > Marine Wing Communications Squadron 18
Marine Wing Communications Squadron 28	Cherry Point, NC	CO MACG 28	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Air Control Group 28 > Marine Wing Communications Squadron 28
Marine Wing Communications Squadron 38	MCAS Miramar, CA	CO MACG-38	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Air Control Group 38 > Marine Wing Communications Squadron 38

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Marine Wing Headquarters Squadron 1	Okinawa, Japan	CG 1 MAW	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Wing Headquarters Squadron 1
Marine Wing Headquarters Squadron 2	Cherry Point, NC	CG 2 MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Wing Headquarters Squadron 2
Marine Wing Headquarters Squadron 3	MCAS Miramar, CA	CG 3 MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Wing Headquarters Squadron 3
Marine Wing Support Group 17	Okinawa, Japan	CG 1 MAW	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Wing Support Group 17
Marine Wing Support Group 27	Cherry Point, NC	CG 2 MAW	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Wing Support Group 27
Marine Wing Support Group 37	MCAS Miramar, CA	CG 3d MAW	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Wing Support Group 37
Marine Wing Support Group 47	Mt.Clemens, MI	CG 4th MAW	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Wing Support Group 47
Marine Wing Support Squadron 171	Iwakuni, Japan	CO MWSG-17	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Wing Support Group 17 > Marine Wing Support Squadron 171
Marine Wing Support Squadron 172	Japan	CO MWSG-17	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 1st Marine Aircraft Wing > Marine Wing Support Group 17 > Marine Wing Support Squadron 172
Marine Wing Support Squadron 271	Cherry Point, NC	CO MWSG-27	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Wing Support Group 27 > Marine Wing Support Squadron
Marine Wing Support Squadron 272	Jacksonville, NC	CO MWSG-27	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Wing Support Group 27 > Marine Wing Support Squadron 272
Marine Wing Support Squadron 273	Beaufort, SC	CO MWSG-27	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Wing Support Group 27 > Marine Wing Support Squadron 273
Marine Wing Support Squadron 274	Cherry Point, NC	CO MWSG-27	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Aircraft Wing > Marine Wing Support Group 27 > Marine Wing Support Squadron 274
Marine Wing Support Squadron 371	Yuma, AZ	CO MWSS-37	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Wing Support Group 37 > Marine Wing Support Squadron 371
Marine Wing Support Squadron 372	Camp Pendleton, CA	CO MWSS-37	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Wing Support Group 37 > Marine Wing Support Squadron 372
Marine Wing Support Squadron 373	MCAS Miramar, CA	CO MWSS-37	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Wing Support Group 37 > Marine Wing Support Squadron 373
Marine Wing Support Squadron 374	29 Palms, CA	CO MWSS-37	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 3rd Marine Aircraft Wing > Marine Wing Support Group 37 > Marine Wing Support Squadron 374
Marine Wing Support Squadron (MWSS) 471	Minneapolis, MN	CO MAG-47	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Wing Support Group 47 > Marine Wing Support Squadron 471
Marine Wing Support Squadron 472	Willow Grove, PA	CO MAG-47	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Wing Support Group 47 > Marine Wing Support Squadron 472
Marine Wing Support Squadron 473	MCAS Miramar, CA	CO MAG-47	RNOSC-PAC	MITSC West	Marine Forces Reserve > 4th Marine Aircraft Wing > Marine Wing Support Group 47 > Marine Wing Support Squadron 473
Marksmanship Center of Excellence	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Marksmanship Center of Excellence
MCAF Meteorology and	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > MCAF Meteorology and Oceanographic

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Oceanographic Division					Division
MCEITS Enterprise Information Technology Center (EITC) Albany	MCNOSC	Albany, GA	MCNOSC	MCNOSC	Marine Forces US Strategic Command > Marine Corps Network Operations and Security Center > MCEITS Enterprise Information Technology Center (EITC) Albany
MCEITS Enterprise Information Technology Center (EITC) Kansas City	MCNOSC	Kansas City, MO	MCNOSC	MCNOSC	Marine Forces US Strategic Command > Marine Corps Network Operations and Security Center > MCEITS Enterprise Information Technology Center (EITC) Kansas City
Military Police Company A (MP Co. A), H&S BN	Lexington, KY	CO H&S BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Military Police Company A
Military Police Company B (MP Co. B), H&S BN	North Versailles, PA	CO H&S BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Military Police Company B
Military Police Company C (MP Co. C), H&S BN	Dayton, OH	CO H&S BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > Headquarters & Service Battalion > Military Police Company C
Military Police Company (MP Co.), HQBN	Minneapolis, MN	CO HQBN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > Headquarters Battalion > Military Police Company
Mountain Warfare Training School (MWTS)	Bridgeport, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > Mountain Warfare Training School
Multi National Force - West (MNF-WIRAQ)	Iraq	CG I MEF	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > Multi National Force - West
Navy-Marine Corps Relief Society	Quantico, VA	CG MCCDC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Base Quantico > Navy-Marine Corps Relief Society
New York City Public Affairs	New York, NY	Dir, Public Affairs	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Division of Public Affairs > Branches > New York City Public Affairs
Office of Legislative Affairs	Washington, DC	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Office of Legislative Affairs
Officer Candidate School (OCS)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Officer Candidate School
Ordinance Maintenance Company (ORDMACO), 4th MAINT BN	Waco, TX	CO 4th MAINT BN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Logistics Group > 4th Maintenance Battalion > Ordinance Maintenance Company
Other Programs of Record (PoR)	VA	CG MCSC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Marine Corps Systems Command > Other Programs of Record
Personal and Family Readiness Division (MR)	Quantico, VA	Dir, M&RA	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Manpower & Reserve Affairs > Personal and Family Readiness Division > Marine Corps Community Services
Plans, Policies & Operations (PP&O)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Plans, Policies & Operations
Programs & Resources (P&R)	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Programs & Resources
Recruiting Station Albany	Albany, NY	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station Albany
Recruiting Station Albuquerque	Albuquerque, NM	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Albuquerque
Recruiting Station Atlanta	Atlanta, GA	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting Station Atlanta
Recruiting Station Baltimore	Baltimore, MD	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Baltimore
Recruiting Station Baton Rouge	Baton Rouge, LA	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
					Station Baton Rouge
Recruiting Station Buffalo	Buffalo, NY	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station Buffalo
Recruiting Station Charleston	Charleston, SC	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Charleston
Recruiting Station Chicago	Chicago, IL	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Chicago
Recruiting Station Cleveland	Cleveland, OH	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Cleveland
Recruiting Station Columbia	Columbia, SC	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting Station Columbia
Recruiting Station Dallas	Dallas, TX	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Dallas
Recruiting Station Denver	Denver, CO	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Denver
Recruiting Station Des Moines	Des Moines, IA	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Des Moines
Recruiting Station Fort Worth	Fort Worth, TX	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Fort Worth
Recruiting Station Ft. Lauderdale	Ft. Lauderdale, FL	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting Station Ft. Lauderdale
Recruiting Station Harrisburg	Harrisburg, PA	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station Harrisburg
Recruiting Station Houston	Houston, TX	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Houston
Recruiting Station Indianapolis	Indianapolis, IN	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Indianapolis
Recruiting Station Indianapolis	Troy, MI	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Troy
Recruiting Station Jacksonville	Jacksonville, FL	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting Station Jacksonville
Recruiting Station Kansas City	Kansas City, MO	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Kansas City
Recruiting Station Lansing	Lansing, MI	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Lansing
Recruiting Station Los Angeles	Los Angeles, CA	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station Los Angeles
Recruiting Station Louisville	Louisville, KY	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Louisville
Recruiting Station Milwaukee	Milwaukee, WI	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Milwaukee
Recruiting Station Montgomery	Montgomery, AL	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
					Station Montgomery
Recruiting Station Nashville	Nashville, TN	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting Station Nashville
Recruiting Station New York	New York, NY	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station New York
Recruiting Station Oklahoma City	Oklahoma City, OK	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Oklahoma City
Recruiting Station Orange County	Orange Co, CA	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station Orange County
Recruiting Station Orlando	Orlando, FL	CO 6MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 6th Marine Corps District > Recruiting Station Orlando
Recruiting Station Phoenix	Phoenix, AZ	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station Phoenix
Recruiting Station Pittsburgh	Pittsburgh, PA	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station Pittsburgh
Recruiting Station Portland	Portland, OR	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station Portland
Recruiting Station Portsmouth	Portsmouth, NH	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station Portsmouth
Recruiting Station Raleigh	Raleigh, NC	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Raleigh
Recruiting Station Richmond	Richmond, VA	CO 4MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 4th Marine Corps District > Recruiting Station Richmond
Recruiting Station Sacramento	Sacramento, CA	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station Sacramento
Recruiting Station Salt Lake City	Salt Lake City, UT	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station Salt Lake City
Recruiting Station San Antonio	San Antonio, TX	CO 8MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 8th Marine Corps District > Recruiting Station San Antonio
Recruiting Station San Diego	San Diego, CA	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station San Diego
Recruiting Station San Francisco	San Francisco, CA	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station San Francisco
Recruiting Station Seattle	Seattle, WA	CO 12MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 12th Marine Corps District > Recruiting Station Seattle
Recruiting Station Springfield	Springfield, MA	CO 1MCD	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Marine Corps Recruiting Command > 1st Marine Corps District > Recruiting Station Springfield
Recruiting Station St. Louis	St. Louis, IL	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station St. Louis
Recruiting Station Twin Cities	Fort Snelling, MN	CO 9MCD	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Marine Corps Recruiting Command > 9th Marine Corps District > Recruiting Station Twin Cities
Regimental Combat Team 1	Camp Pendleton, CA	CO 1st Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 1st Marine Regiment >

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
					Regimental Combat Team 1
Regimental Combat Team 5	Camp Pendleton, CA	CO 5th Marines	RNOSC-PAC	MITSC West	Marine Forces Pacific > I Marine Expeditionary Force > 1st Marine Division > 5th Marine Regiment > Regimental Combat Team 5
Regimental Combat Team 8	Camp Lejeune, NC	CO 8th Marines	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > 2nd Marine Division > 8th Marine Regiment > Regimental Combat Team 8
Safety Division	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Safety Division
School of Infantry - East (SOI East)	Camp Lejeune, NC	CG TECOM	RNOSC-LANT	MITSC East	Headquarters Marine Corps > Training & Education Command > School of Infantry-East
School of Infantry - West (SOI West)	Camp Pendleton, CA	CG TECOM	RNOSC-PAC	MITSC West	Headquarters Marine Corps > Training & Education Command > School of Infantry-West
Sergeant Major of the Marine Corps	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Sergeant Major of the Marine Corps
Site R	xxx	CMC	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Site R
Special Operations Training Group	Camp Lejeune, NC	CG II MEF	RNOSC-LANT	MITSC East	Marine Forces Command > II Marine Expeditionary Force > Special Operations Training Group
Special Operations Training Group	Okinawa, Japan	CG III MEF	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > Special Operations Training Group
Special Purpose Marine Air-Ground Task Force Afghanistan	Afghanistan	COMMARFOR CENT	N/A	N/A	Marine Forces Central > Special Purpose Marine Air-Ground Task Force Afghanistan
Staff Judge Advocate to the Commandant	Arlington, VA	CMC	RNOSC-NCR	MITSC HQMC	Headquarters Marine Corps > Staff Judge Advocate to the Commandant
TOW Company (Anti-Armor Tube-launched, optically tracked, wire guided missile), 4th MARDIV	Broken Arrow, OK	CG 4th MARDIV	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > TOW Company
Train The Trainer School (T3S)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Train The Trainer School
Training & Education Command (TECOM)	Quantico, VA	DC CD&I	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command
Truck Company, HQBN	Ebensburg, PA	CO HQBN	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > Headquarters Battalion, Truck Company
Technical Services Organization (TSO) – Kansas City	Kansas City, MO	HQMC/PR	RNOSC-NCR	MITSC HQMC / TSO-KC	Headquarters Marine Corps > Programs & Resources> Technical Services Organization
Technical Services Organization (TSO) – Indianapolis	Indianapolis, IN	HQMC/PR	RNOSC-NCR	MITSC HQMC / TSO-IND	Headquarters Marine Corps > Programs & Resources>Technical Services Organization
U.S. Marine Corps Forces, Special Operations Command	Camp Lejeune, NC	CMC & Cmdr USSOCOM	RNOSC-LANT	MITSC East	U.S. Marine Corps Forces, Special Operations Command
Unit Deployment Battalion	Japan	CO 4th Marines	RNOSC-PAC	MITSC WestPac	Marine Forces Pacific > III Marine Expeditionary Force > 3rd Marine Division > 4th Marine Regiment > Unit Deployment
Weapons and Rifle Platoon (WPN & RFL PLT), F Co, 2/23	Las Vegas, NV	CO F Co	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 3rd Battalion, 23rd Marines > F Company > Weapons and Rifle Platoon
Weapons Company, 1/23	Austin, TX	CO 1/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 1st Battalion > Weapons Company

Unit	Garrison Location	C2 Reporting To	RNOSC	MITSC	C2 Organization Hierarchy
Weapons Company, 1/24	Perrysburg, OH	CO 1/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 1st Battalion > Weapons Company
Weapons Company, 1/25	Devens, MA	CO 1/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 1st Battalion > Weapons Company
Weapons Company, 2/23	Port Hueneme, CA	CO 2/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 2nd Battalion > Weapons Company
Weapons Company, 2/24	Waukegan, IL	CO 2/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 2nd Battalion > Weapons Company
Weapons Company, 2/25	Garden City, NY	CO 2/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 2nd Battalion > Weapons Company
Weapons Company, 3/23	Baton Rouge, LA	CO 3/23	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 23rd Marine Regiment > 3rd Battalion > Weapons Company
Weapons Company, 3/24	Springfield, MO	CO 3/24	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 24th Marine Regiment > 3rd Battalion > Weapons Company
Weapons Company, 3/25	Akron, OH	CO 3/25	RNOSC-RES	MITSC Reserves	Marine Forces Reserve > 4th Marine Division > 25th Marine Regiment > 3rd Battalion > Weapons Company
Weapons Training Battalion (WTBN)	Quantico, VA	CG TECOM	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Training & Education Command > Weapons Training Battalion
Wounded Warrior Regiment (WWR)	Quantico, VA	Dir, M&RA	RNOSC-NCR	MITSC NCR	Headquarters Marine Corps > Manpower & Reserve Affairs > Wounded Warrior Regiment

(This page intentionally left blank)