Marine Corps Information Enterprise (MCIENT) Strategy

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS
Headquarters, U.S. Marine Corps, Washington, DC
C4

14 DEC 2010

DOCUMENT CHANGE RECORD

Version Number	Date	Description
V 0.1	April 19, 2010	Pre-Decisional Draft Release
V 0.2	July 23, 2010	Pre-Decisional Draft Release
V 0.3	September 15, 2010	Pre-Decisional Draft Release
V 1.0	December 14, 2010	First Release

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

The Marine Corps will continue to meet the challenges of a complex security environment, fight and win our Nation's battles, and endure as the Nation's expeditionary force in readiness. To ensure these imperatives, we will evolve our Corps into a *Knowledge-based Force* that achieves decision and execution superiority, leverages seamless communications for decisive advantage, and extends our Corps' warfighting preeminence into Cyberspace. The Marine Corps Information Enterprise (MCIENT) Strategy prepares our Corps for the future by establishing a vision for the Marine Corps as an *Information Enterprise* and by providing the objectives necessary for enhancing our Service core competencies, defeating our adversaries, supporting our allies and mission partners, and performing our legislated role.

Winning the Nation's battles and succeeding in complex security environments demands we operate as effectively in Cyberspace as we do in traditional warfighting domains and business mission areas. This requires the Marine Corps to evolve into a Knowledge-based Force that can bring knowledge to bear for decision and execution superiority. To this end, we must enhance our Marine Corps Enterprise Network (MCEN), ensuring its ability to securely and rapidly deliver a robust and seamless Marine Corps Information Environment (MCIE). We must influence and rapidly infuse emerging technologies that enhance Command and Control (C2), extend the reach of forward deployed forces, and improve organizational and tactical agility. Additionally, to ensure we continue providing superior expeditionary capabilities to Combatant Commanders, we must govern the enterprise through regionally responsive governance practices that enable us to forward stage and provide mission critical data, information, and knowledge to bandwidth limited Marines and mission partners. This requires effective technical solutions and a workforce that knows how to use improved governance tools, policies, and enterprise capabilities to create advantage in a dynamic strategic landscape. Finally, we must infuse within Marine Corps Cyberspace practices an institutionalized Information Assurance (IA) capability to ensure we value and protect information and knowledge as decisive strategic assets.

As state and non-state actors complicate the global security environment by blurring traditional and irregular capabilities and tactics, our Corps will evolve into a *Knowledge-based Force* that harnesses seamless communications across the *Information Enterprise* to achieve decision and execution superiority in all warfighting domains and business mission areas. This strategy provides an essential contribution to the growing body of guidance and current strategic planning initiatives shaping our Corps to meet the threats and challenges of a dynamic strategic landscape. In the end, the Marine Corps will operate as a strategically attuned, responsive, and agile force that excels as the Nation's expeditionary force in readiness.

Kevin J. Nally
Brigadier General, U.S. Marine Corps
Director Command, Control, Communications, and Computers (C4)

Page intentionally left blank

1 INTRODUCTION

The Commandant of the Marine Corps (CMC) directed the development of the *Marine Corps Information Enterprise (MCIENT) Strategy* in order to posture the Marine Corps to meet the challenges of the future security environment. The Director Command, Control, Communications, and Computers (Director C4) / Department of the Navy Deputy Chief Information Officer, Marine Corps (DDCIO (MC)), in coordination with others, developed the MCIENT Strategy to inform the direction of future enterprise capabilities in support of the Force Development process. The MCIENT Strategy serves as Appendix 1 to Annex K of the Marine Corps Service Campaign Plan (SCP). As an appendix to the Service Campaign Plan, this document provides CMC authorized guidance for the MCIENT.

1.1 STRATEGIC IMPERATIVE

The MCIENT Strategy facilitates Marine Corps tactical, operational, and strategic advantage by evolving the Marine Corps into a ***Knowledge-based Force*** that: (1) achieves decision and execution superiority, (2) leverages seamless communications for decisive advantage, (3) and extends the Corps' warfighting preeminence into Cyberspace. This imperative is served through the enhancement of our Service core competencies and through the effective use of people, processes, information, and technology across the organization, in Cyberspace, and in all warfighting domains and business mission areas.

1.2 PURPOSE

The *Marine Corps Information Enterprise Strategy* influences enterprise Force Development priorities by providing the Marine Corps' single, top level Information Enterprise objectives that inform future capability decisions, supporting plans, concepts, and programming initiatives. The strategy does not seek changes to existing institutional processes, but rather seeks to become integral to their prescribed courses by establishing a prioritized set of enterprise objectives used as input to senior leader Force Development guidance. Furthermore, the MCIENT Strategy presents a conceptual model for the Marine Corps as an *Information Enterprise*, consistent with the DOD Information Enterprise (DOD IE) concept and Joint Cyberspace operational concepts. The model provides the Director C4 / DDCIO (MC) with a framework for coordinating the development of Information Enterprise objectives, integrated Advocate Roadmaps, and Service level policies derived from MCIENT requirements. To ensure clarity and consistency across the Corps, all other Information Enterprise or applicable Cyberspace related capability descriptions, strategies, concepts, policies, plans, initiatives, manuals, or any other product, should be written in support of, or in coordination with this document's vision and objectives.

1.3 METHOD

The MCIENT Strategy is the product of a four step Strategy Development and Lifecycle Management Process. This process is grounded in the Marine Corps Planning Process (MCPP) and the ends – ways – means construct described in MCDP 1-1, *Strategy*. The four step process depicted in Figure 1 is designed to provide the Director C4 / DDCIO (MC) with a continuous and structured method for coordinating the development of Information Enterprise objectives that achieve the strategy's vision and inform Force Development priorities. Furthermore, the Strategy Development and Lifecycle Management Process provides a mechanism for the Director C4 / DDCIO (MC) to facilitate the integration of Advocate Roadmaps, consistent with Information Enterprise objectives. Finally, the process ensures this MCIENT Strategy and future updates are: (1) *developed* in support of Marine Corps institutional objectives, (2) *communicated* across the Corps and to external audiences, (3) *executed* by the organization, and (4) are *assessed* and *reviewed* for relevance and for implementation success. Figure 1 depicts the cyclical process in use to develop and execute this strategy.

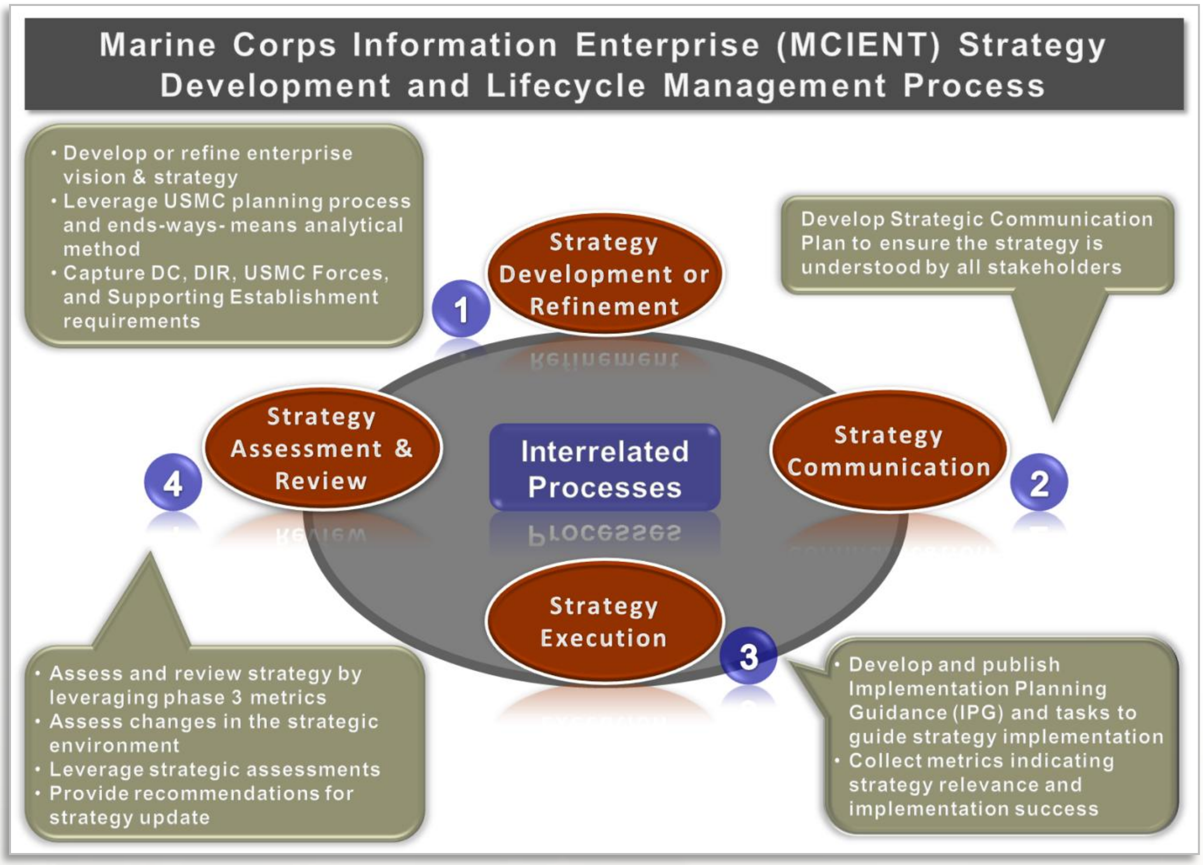

Marine Corps Information Enterprise (MCIENT) Strategy Development and Lifecycle Management Process
• Develop or refine enterprise vision & strategy
• Leverage USMC planning process and ends-ways- means analytical method
• Capture DC, DIR, USMC Forces, and Supporting Establishment requirements
1
Strategy Development or Refinement
Develop Strategic Communication Plan to ensure the strategy is understood by all stakeholders
Strategy Communication
2
Interrelated Processes
Strategy Assessment & Review
4
Strategy Execution
3
• Develop and publish Implementation Planning Guidance (IPG) and tasks to guide strategy implementation
• Collect metrics indicating strategy relevance and implementation success
• Assess and review strategy by leveraging phase 3 metrics
• Assess changes in the strategic environment
• Leverage strategic assessments
• Provide recommendations for strategy update

Figure 1. MCIENT Strategy Development & Lifecycle Process

Phase 1: the MCIENT Strategy Development or Refinement phase is the first phase of the overall processes. During phase 1, the Director C4 / DDCIO (MC) develops or revises the base strategy document by leveraging maximum stakeholder participation, the Marine Corps Planning Process (MCPP), and by using the ends – ways – means construct described in MCDP 1-1, Strategy. During phase 1, the Director C4 / DDCIO (MC) coordinates the analysis of the strategic environment and Information Enterprise requirements from Deputy Commandants, Directors, Marine Corps Forces, and the Supporting Establishment. Leveraging analysis results, and maximum stakeholder participation, the Director C4 / DDCIO (MC) drafts and publishes the base MCIENT Strategy document or its revision to complete phase 1.

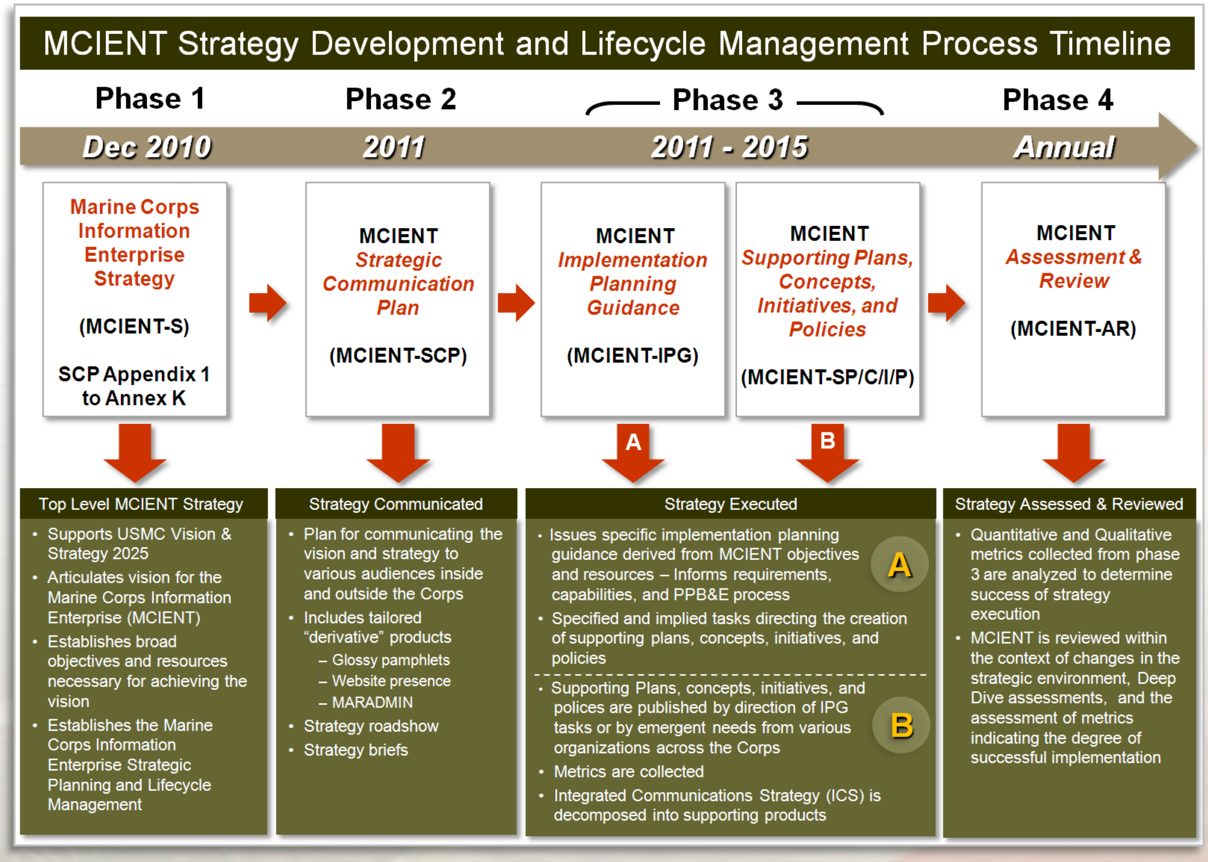
Phase 2: the MCIENT Strategy Communication phase ensures the strategy is communicated across the Marine Corps and to external audiences and mission partners through a comprehensive strategic communication plan. Under this plan, the Director C4 / DDCIO (MC) produces tailored products to communicate specific strategy elements and objectives to specific audiences via multiple means (e.g., presentations, glossy prints, website, etc.). The intent of phase 2 is to ensure the MCIENT Strategy is well understood and accepted by stakeholders inside and outside the Marine Corps. The activities of phase 2 are continuous and span all other phases of the Strategy Development and Lifecycle Management Process.

Phase 3: the MCIENT Strategy Execution phase begins with the development of Implementation Planning Guidance (IPG) and tasks. During phase 3 the Director C4 / DDCIO (MC) hosts an Implementation Planning Conference with implementation stakeholders to develop the guidance and tasks necessary for strategy achievement. Because this phase spans the strategy’s lifecycle, it becomes a continuous coordination and oversight process that integrates into established force development, resourcing, and lifecycle management activities performed by other USMC organizations. Finally, phase 3 requires the implementation and use of quantitative and qualitative metrics useful for determining strategy relevance and implementation success. Data created during phase 3 will be gathered and evaluated during phase 4.

Phase 4: the MCIENT Strategy Assessment and Review phase requires strategy assessors to combine metrics gathered from phase 3 with other strategic assessments to determine the strategy's degree of implementation success, as well as the document's relevance to changes in the strategic landscape. This phase is related to but is not the same as measuring the value of specific IT investments as a function of the Capital Planning and Investment Control (CPIC) process. Instead, phase 4 regards the strategy itself as a product and a process that helps shape the force through specific enterprise objectives and priorities. Therefore, phase 4 should be conducted annually and in synchronization with CMC level Force Development guidance. Phase 4 completes the Strategy Development and Lifecycle Management process by providing output products that return the cycle to phase 1.

1.4 MCIENT STRATEGY AND ASSOCIATED PRODUCTS TIMELINE

Figure 2 associates the cyclical Strategy Development and Lifecycle Management Process identified in Figure 1 with a timeline applicable for this document and its associated derivative products. Publishing the MCIENT Strategy represents phase 1 completion.



MCIENT Strategy Development and Lifecycle Management Process Timeline

Phase 1 — Dec 2010

Marine Corps Information Enterprise Strategy

(MCIENT-S)

SCP Appendix 1 to Annex K

Top Level MCIENT Strategy

- Supports USMC Vision & Strategy 2025
- Articulates vision for the Marine Corps Information Enterprise (MCIENT)
- Establishes broad objectives and resources necessary for achieving the vision
- Establishes the Marine Corps Information Enterprise Strategic Planning and Lifecycle Management

Phase 2 — 2011

MCIENT Strategic Communication Plan

(MCIENT-SCP)

Strategy Communicated

- Plan for communicating the vision and strategy to various audiences inside and outside the Corps
- Includes tailored "derivative" products
  - Glossy pamphlets
  - Website presence
  - MARADMIN
- Strategy roadshow
- Strategy briefs

Phase 3 — 2011 - 2015

MCIENT Implementation Planning Guidance

(MCIENT-IPG)

A

MCIENT Supporting Plans, Concepts, Initiatives, and Policies

(MCIENT-SP/C/I/P)

B

Strategy Executed

- Issues specific implementation planning guidance derived from MCIENT objectives and resources – Informs requirements, capabilities, and PPB&E process
- Specified and implied tasks directing the creation of supporting plans, concepts, initiatives, and policies

A

- Supporting Plans, concepts, initiatives, and polices are published by direction of IPG tasks or by emergent needs from various organizations across the Corps
- Metrics are collected
- Integrated Communications Strategy (ICS) is decomposed into supporting products

B

Phase 4 — Annual

MCIENT Assessment & Review

(MCIENT-AR)

Strategy Assessed & Reviewed

- Quantitative and Qualitative metrics collected from phase 3 are analyzed to determine success of strategy execution
- MCIENT is reviewed within the context of changes in the strategic environment, Deep Dive assessments, and the assessment of metrics indicating the degree of successful implementation

Figure 2. MCIENT Strategy Development and Execution Timeline

1.5 MCIENT DEFINITION

The Marine Corps Information Enterprise (MCIENT) is defined as the Marine Corps information resources, assets, services, and processes required to achieve decision and execution superiority and to share information and knowledge across the Marine Corps and with mission partners. It includes the following components: (a) the Marine Corps Enterprise Network (MCEN), (b) the Marine Corps Information Technology Environment (MCITE), (c) the Marine Corps Information Environment (MCIE), (d) Cyberspace Operations – grounded in a defense-in-depth strategy, (e) IT Service Management (ITSM), (f) USMC institutional processes, organizations, and personnel, and (g) Enterprise Architecture (EA). Figure 3 depicts the interrelation of components that form the Marine Corps Information Enterprise model. In sum, the Marine Corps Information Enterprise Model represents the Marine Corps viewed as an Information Enterprise. The model provides the Director C4 / DDCIO (MC) with useful coordination framework for facilitating the integration of objectives and plans across the enterprise.

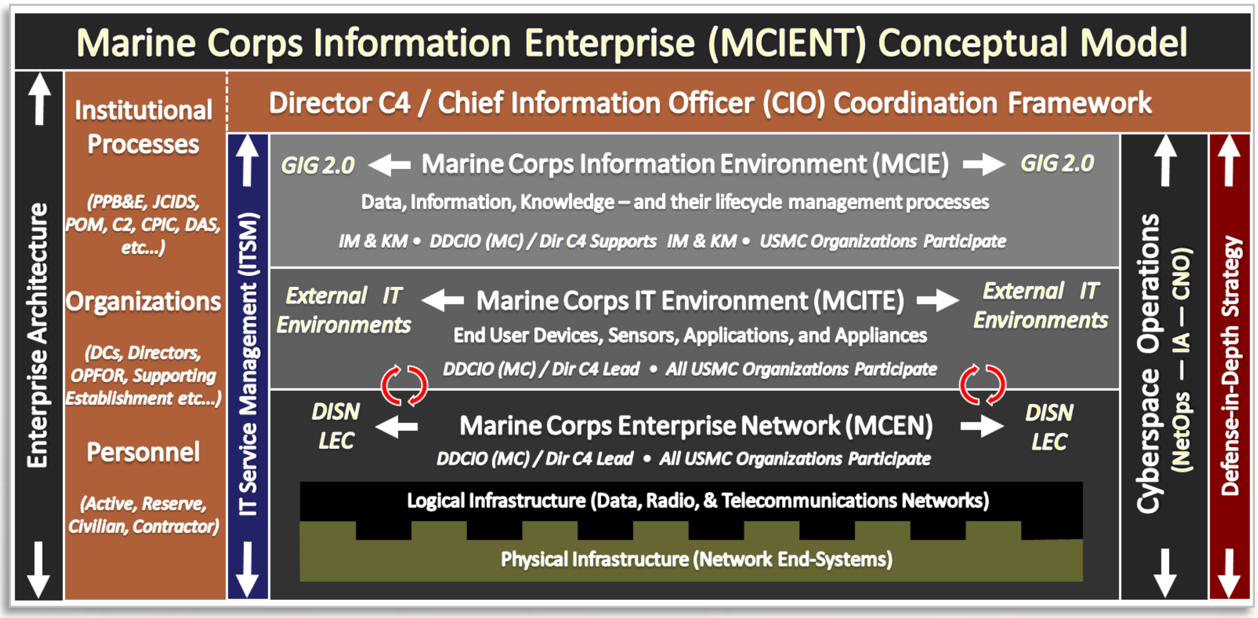

Marine Corps Information Enterprise (MCIENT) Conceptual Model
Enterprise Architecture
Institutional Processes
(PPB&E, JCIDS, POM, C2, CPIC, DAS, etc...)
Organizations
(DCs, Directors, OPFOR, Supporting Establishment etc...)
Personnel
(Active, Reserve, Civilian, Contractor)
Director C4 / Chief Information Officer (CIO) Coordination Framework
IT Service Management (ITSM)
GIG 2.0
Marine Corps Information Environment (MCIE)
GIG 2.0
Data, Information, Knowledge – and their lifecycle management processes
IM & KM • DDCIO (MC) / Dir C4 Supports IM & KM • USMC Organizations Participate
External IT Environments
Marine Corps IT Environment (MCITE)
External IT Environments
End User Devices, Sensors, Applications, and Appliances
DDCIO (MC) / Dir C4 Lead • All USMC Organizations Participate
DISN LEC
Marine Corps Enterprise Network (MCEN)
DISN LEC
DDCIO (MC) / Dir C4 Lead • All USMC Organizations Participate
Logical Infrastructure (Data, Radio, & Telecommunications Networks)
Physical Infrastructure (Network End-Systems)
Cyberspace Operations
(NetOps — IA — CNO)
Defense-in-Depth Strategy

Figure 3. Marine Corps Information Enterprise (MCIENT)

The MCIENT model supports the broader Department of Defense (DOD) Information Enterprise (IE) concept as defined in DODD 8000.01 – Management of the Department of Defense Information Enterprise, Joint Cyberspace Operations concepts and definitions, and DODI 8410.02 – NetOps for the Global Information Grid (GIG). All Marine Corps institutional processes, organizations, and personnel are part of the MCIENT conceptual model because they lead, support, or leverage one or more of the model's core components or component interactions.

1.5.1 Marine Corps Enterprise Network (MCEN)

At the core of the MCIENT model is the Marine Corps Enterprise Network (MCEN). The MCEN is defined as:

> **The Marine Corps' network-of-networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations.**

Figure 4. Marine Corps Enterprise Network (MCEN) Definition

The MCEN is characterized at a minimum to include: (1) **Programs of Record (PORs)** that provide network services to forward deployed forces (e.g., DDSM, LMST, Phoenix, SWAN, etc.) operating in the USMC.mil namespace and in USMC routable IP addresses, and (2) **Operations and Maintenance (O&M)** functions that provision data transportation, enterprise IT, network services, and boundary defense (e.g., MCEITS, NGEN, SONIC, etc.).

Additionally, the MCEN's physical infrastructure is analogous to the Defense Information System Network (DISN), and the Local Exchange Carrier (LEC), as it enables the Marine Corps Information Technology Environment (MCITE) and the flow of data, information, and knowledge across the Marine Corps Information Environment (MCIE). The

MCEN interfaces with external networks to provide information and resource sharing, as well as access to external services.

Finally, when end user devices, sensors, applications, and appliances are connected to the MCEN, they become part of the network through a relationship established at an interface point. Interfaces, as indicated by the circular arrows connecting the MCEN and MCITE in Figure 3, represent an important feature of the model that must be managed effectively to ensure component layer integration. Each MCIENT component layer contributes to the next higher layer by providing services through an approved interface.

1.5.2 Marine Corps Information Technology Environment (MCITE)

Figure 3 depicts the MCEN and MCITE as inextricably linked, but distinguishes the MCITE layer as that which encompasses all Marine Corps owned and operated IT – including those technologies inherent and not inherent to the MCEN's core operation. Information Technologies directly associated with operating the MCEN's logical and physical infrastructure are always considered an inherent part of the MCEN’s core operation, and are always considered a permanent portion of the MCITE.

However, Information Technologies not associated with the MCEN’s core operation (e.g., Smart Phones, DDS-M, GCSS-MC, AFATDS, GCCS, IOSV3, IOW, JTCW, CAC2S, JBCP, and all end systems) are considered ancillary and are therefore only considered a part of the MCEN when they are connected to it through an approved interface. Like inherent MCEN technologies, ancillary technologies are always considered a permanent portion of the MCITE. The circular arrows in Figure 3 indicate the inextricable but often ephemeral link between the MCEN and the MCITE. This distinction and relationship is important to note in order to highlight the intent of the MCITE layer as an encompassing construct around all Marine Corps IT, whether inherent to the MCEN or ancillary to it. This distinction is essential for policy matters and architecture initiatives.

1.5.3 Marine Corps Information Environment (MCIE)

The MCIE represents the broad domain for all forms of communication. It comprises Marine Corps data, information, knowledge, and the management processes for ensuring their effective distribution and use across the Marine Corps and with mission partners. The MCIE often leverages, but does not always depend upon technology and communications systems to facilitate the flow of data, information, and knowledge across the enterprise. **Therefore, the MCIE represents a broad domain within which all communication takes place (e.g., explicit and implicit communications). Within the MCIE data, information, and knowledge is shared, situational understanding is achieved, and decisions are made.**

1.5.4 Cyberspace Operations and Defense-in-Depth Strategy

Joint Publication (JP) 1-02 defines Cyberspace Operations as *“*The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through Cyberspace. Such operations include Computer Network Operations (CNO) and activities to operate and defend the Global Information Grid*”.* According to the Marine Corps Cyberspace Concept 2009, Cyberspace Operations can be divided into three broad categories: **Network Operations (NetOps)**, **Information Assurance (IA)**, and **CNO**.

Figure 3 depicts Cyberspace Operations as applicable to the three core layers of the MCIENT model. Therefore, the planning, development, and management of future Marine Corps cyberspace capabilities and operations should be conducted within the context of the model. Various USMC stakeholder organizations including but not limited to: Marine Forces Cyber Command (MARFORCYBER), Deputy Commandant for Combat Development and Integration (DC CD&I) Cyber Integration Division, Director C4 / DDCIO (MC), and the Marine Corps Network Operations Security Center (MCNOSC) each play a key role in developing, managing, or operating various aspects of cyberspace policy or capabilities as they apply to the MCIENT model. Figure 3 serves to illustrate, from an institutional perspective, the need for Marine Corps cyberspace stakeholders to coordinate closely in the development, management, and operation of cyberspace capabilities.

Figure 3 also indicates that USMC Cyberspace Operations are made more effective by grounding in an institutional defense-in-depth strategy. The Committee on National Security Systems (CNSS) Instruction No. 4009, 2006 defines defense-in-depth as an “IA strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of networks.” Figure 3 implies this strategy is applicable across the three core layers of the MCIENT including the MCEN, MCITE, and MCIE. While the definition is largely focused on “networks” this strategy broadens the definition’s scope to ensure we plan to incorporate future concepts and policies from an enterprise perspective that provide protective measures across the three core layers.

1.5.5 Network Operations (NetOps)

The Marine Corps’ concept for NetOps is consistent with the DoDI 8410.02, *NetOps for the Global Information Grid (GIG)* dated December 19th, 2008. Figure 3 depicts USMC NetOps as a component of Cyberspace Operations applicable to the three core MCIENT components (i.e., MCEN, MCITE, and MCIE). Therefore, the planning, development, and management of future Marine Corps NetOps capabilities and operations should be conducted within the context of the model. USMC NetOps is defined as the Marine Corps-wide operational, organizational, and technical capabilities for operating and defending the MCIENT core components. NetOps includes, but is not limited to, enterprise management, net assurance, and content management. NetOps provides commanders with MCIENT situational awareness to make informed command and control decisions. MCIENT situational awareness is gained through the operational and technical integration of enterprise management and defense actions and activities across all levels of command (strategic, operational, and tactical).

1.5.6 Information Assurance (IA)

The Marine Corps’ concept for Information Assurance is consistent with the JP 1-02, *DoD Dictionary of Military and Associated Terms* definition for Information Assurance (IA). The Joint Publication defines IA as the “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” Marine Corps IA seeks to ensure cyberspace policies, procedures, standards, and methodologies are implemented to guarantee information delivery, data integrity, and to ensure information protection. Marine Corps IA ensures end-to-end capability to deliver secure information at the right time, to the right place, and in a usable format, allowing commanders to exercise command and communication, regardless of the proximity to their assigned forces.

IA is a broad discipline that includes policies and operational activities performed by various organizations and skilled personnel across the Marine Corps in order to protect and defend our information and information systems. As a subset of Cyberspace Operations in Figure 3, IA finds applicability to the three core layers of the MCIENT. Therefore, the planning, development, and management of future Marine Corps Information Assurance capabilities and operations should be conducted within the context of the model and the IA objectives set forth by this strategy.

1.5.7 Computer Network Operations (CNO)

The Marine Corps’ concept for CNO is consistent with the JP 1-02 definition for CNO. Figure 3 depicts CNO as a subset of Cyber Operations applicable to the three core layers of the MCIENT model. Therefore, the planning, development, and management of future Marine Corps CNO capabilities and operations should be conducted within the context of the model.

JP 1-02 characterizes **CNO** as “Comprised of computer network attacks, computer network defense, and related computer network exploitation enabling operations.” **Computer Network Attack (CNA)** includes “Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” **Computer Network Defense (CND)** includes “Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks.” CND employs information assurance (IA) capabilities to respond to unauthorized activity within DoD information systems and computer networks in response to a CND alert or threat information. CND also employs intelligence, counterintelligence, law enforcement, and other military capabilities to defend DoD information and computer networks. **Computer Network Exploitation (CNE)** includes "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."

1.5.8 IT Service Management (ITSM)

ITSM is a NetOps enabler by providing effective, efficient, and responsive delivery of essential IT services to Marine Corps customers and users. This explains the placement of ITSM in Figure 3 between institutional processes, organizations, and personnel and the core component layers. ITSM delivers the capabilities of the core model layers to consumers and users. ITSM represents a framework for specialized functions and processes that provides value to customers and users in the form of IT services. ITSM processes support conceptualization, planning, procurement, implementation, and operation of IT services. Well-defined interfaces ensure the integration of acquisition, governance, and operational IT services activities. The Marine Corps will continue to advance the implementation of ITSM institutionally in support of Knowledge-based Force capabilities.

1.5.9 Institutional Processes, Organizations, and Personnel

The MCIENT Conceptual Model also includes current Marine Corps institutional processes, organizations, and personnel related to the development, operation, and management of core MCIENT components. ***Force Development*** processes include but are not limited to: Capability Based Assessments (CBA), Universal Needs Statements (UNS), Expeditionary Force Development System (EFDS), and the Joint Capabilities Integration and Development System (JCIDS). The MCIENT Strategy Development and Lifecycle Process provides the Director C4 / DCIO (MC) with a framework for advising senior leader guidance delivered at the beginning of the Force Development processes.

Acquisition processes include but are not limited to: the Defense Acquisition System (DAS), and Programming, Budgeting and Execution processes. The Director C4 / DCIO (MC) contributes to acquisition processes by executing Capital Planning and Investment Control (CPIC) responsibilities for enterprise IT initiatives and by reporting IT Steering Group evaluation results to Programmers.

Operation and governance processes include but are not limited to: MCEN NetOps, situational awareness and reporting, and the creation, exchange, management and use data, information, and knowledge. It also includes processes that leverage laws, regulations, and policies to establish organizational authorities, responsibilities, and relationships necessary for implementing and overseeing the development and use of MCIENT components and related Cyberspace Operations. Examples of governance processes include but are not limited to those guiding Chief Information Officer (CIO) activities and other oversight bodies (e.g., Operational Advisory Group (OAG), and IT Steering Group (ITSG), etc.).

1.5.10 Enterprise Architecture (EA) & the Director C4 / CIO Coordination Framework

Finally, the MCIENT model depicts Enterprise Architecture (EA) as an institutional framework and practice that integrates with the Strategy Development and Lifecycle Management Process illustrated by Figure 1. Figure 3 depicts EA on the far left side of the model because its scope is institutional, and its method is comprehensive for planning and synchronizing organizational processes, information, and technology. EA practices, as a function of the CIO Coordination Framework, inform and guide the processes, organizations, and people that develop, acquire, operate, and manage core MCIENT components. **The CIO Coordination Framework exists within this model as a basis for leveraging EA and existing institutional processes, organizations, and people to develop and implement enterprise strategy and objectives in support of the Force Development process.**

1.6 SCOPE

This document is applicable to the MCIENT and its components as depicted in Figure 3. Given the scope, this document calls attention for the need to institutionalize Information Management (IM) and Knowledge Management (KM) practices across the Marine Corps. Because there is currently no comprehensive program or initiative to define, develop, implement, and synchronize IM and KM capabilities and practices across the total force, this document does not provide objectives or recommendations for specific IM and KM concepts, policies, or practices. The Director C4 / DDCIO (MC) will assist deputy commandants, or other organizations charged with implementing IM and KM initiatives by providing a supporting technology environment as required. Similarly, because the development of cyberspace operational concepts, policies, and practices fall under the purview of Marine Forces Cyber Command (MARFORCYBER), this document limits cyberspace objectives to that of protecting and defending cyberspace relevant MCIENT components. The Director C4 / DDCIO (MC), acting in dual capacity as the Deputy Commanding General for MARFORCYBER, will assist CG MARFORCYBER, as required, in the development or implementation of cyberspace capabilities.

2 MCIENT VISION, STRATEGY, AND CHARACTERISTICS

2.1 VISION STATEMENT

> **"I want a Knowledge-based Force that leverages seamless enterprise capabilities across the spectrum of conflict in order to enhance decision making, achieve knowledge superiority, and gain tactical, operational, and strategic advantage over our Nation's adversaries."**
>
> **- Brigadier General Kevin J. Nally, USMC**

Figure 5. MCIENT Vision Statement

2.2 MCIENT STRATEGY SUMMARY

Achieving the vision requires the development of improved mobile, seamless, and secure communications and IT services across the Information Enterprise. Communications and services with these characteristics facilitate collaboration, coordinated actions, and instant or near real time access to mission critical data, information, and knowledge. To evolve the Corps into a Knowledge-based Force that achieves decision and execution superiority in traditional warfighting domains, Cyberspace, and business mission areas, investments in core MCIENT components are crucial. Investments for the Marine Corps Enterprise Network (MCEN) and the Marine Corps Information Technology Environment (MCITE) will focus on ensuring their ability to more effectively deliver, display, and manage data, information, and knowledge across the enterprise.

Furthermore, investments will emphasize better ways for rapidly infusing emerging technologies that enhance Command and Control (C2), extend the reach of forward deployed forces, and improve organizational and tactical agility. Investments will be planned from the perspective of ensuring bandwidth limited Marines and mission partners have improved access to mission critical data, information, and knowledge, wherever and whenever needed, and in an understandable format. Enterprise investments will also focus on workforce education, training, and professionalization programs. Such initiatives will be designed to ensure Marines, Civilian Marines, and support contractors know how to use improved enterprise governance tools, policies, and technological capabilities to create advantage in a dynamic strategic landscape.

Finally, the MCIENT will embody an institutional sense and practice for leveraging, protecting, and defending data, information, and knowledge as decisive strategic assets. To this end, the Marine Corps will infuse within its Cyberspace capabilities an institutionalized Information Assurance (IA) practice for ensuring data, information, and knowledge yield decisive advantage to the Corps, the Nation, and not the enemy.

2.3 MCIENT CHARACTERISTICS

2.3.1 Focused on Deployed Forces

The location of MAGTF or other USMC forward deployed forces in the future will vary depending upon the operating context, mission, and the extent to which Marines interact with internal and external organizations and individual mission partners. In the future, the Marine Corps will leverage multi-capable MAGTFs with Marines who are trained to perform a multitude of tasks in varying operational contexts and at differing levels of unit aggregation. MCIENT components will support these Marines by facilitating the development and fielding of mobile, seamless, and secure communications and IT services that provide robust collaboration tools and instant or near real time access to mission critical data, information, and knowledge.

2.3.2 Attuned to the Strategic Environment

The MCIENT is attuned to the strategic environment by facilitating the development and fielding of tools that help Marines, Civilian Marines, and contractors better assess, adapt to, and influence changes in a dynamic strategic landscape. Attuning the enterprise to the strategic environment requires a special emphasis on leveraging intelligence, including cyber-intelligence, for proactive and reactive mitigation of cyber attacks and threats, and for successful execution of Cyberspace missions across the full spectrum operations.

2.3.3 Grounded in Effective Governance

Effective governance implies a mechanism for ensuring that MCIENT capabilities are developed and fielded in support of Marine Corps goals and objectives. The MCIENT model provides a framework for integrating common functional requirements, applicable to MCIENT components, into enterprise objectives. The *Marine Corps Information Enterprise Strategy* is thus the mechanism for leveraging the MCIENT model to influence enterprise Force Development priorities. The MCIENT strategy provides the Marine Corps' single, top level enterprise objectives used to inform future capability decisions, supporting plans, concepts, and programming initiatives.

2.3.4 Secure and Seamless Marine Corps Information Environment

MCIENT core components enhance the ability for Marines and their mission partners to access the information they need in austere and distributed environments, whenever they need it. The Director C4 / DDCIO (MC) will coordinate with other organizations to define the implementations required for ensuring information is visible, accessible, discoverable, and understandable in a way consistent with the effective use of constrained bandwidth. Additionally, through programs of record and Marine Corps IT regionalization practices, information will be distributed to deployed forces and staged as far forward as required to ensure availability in a bandwidth constrained environment. Structured and unstructured data spanning all functional areas will support the distribution, forward staging, and sharing among all command echelons. Finally, creating a secure and seamless Information Environment requires an Enterprise Architecture (EA) that integrates all Marine Corps components who manage segment architectures within the MCIENT (e.g., Battlespace Awareness, Force Application, etc.).

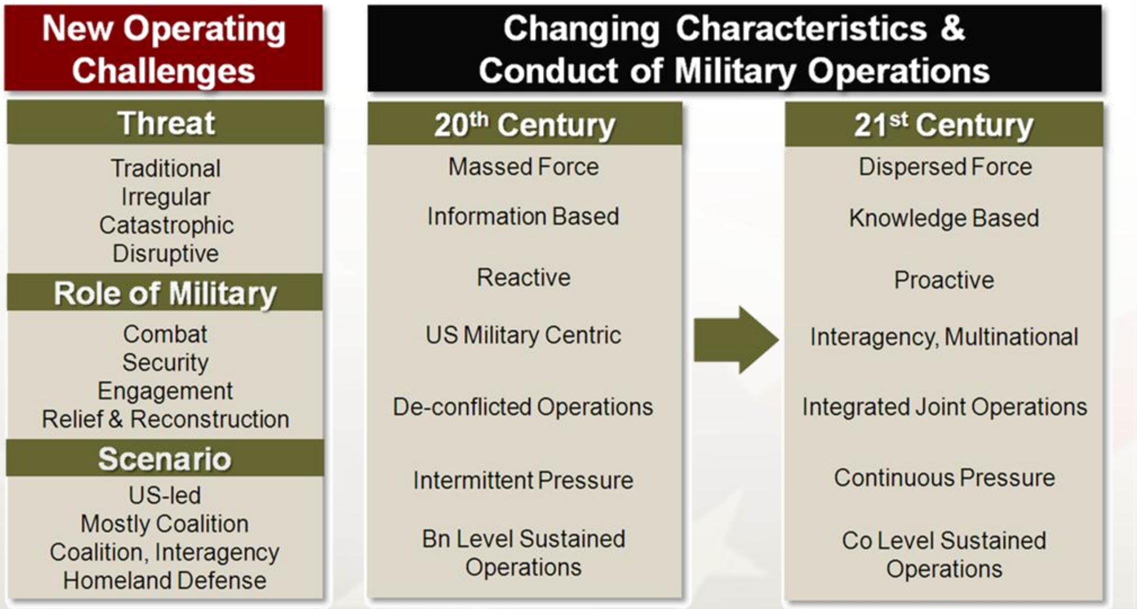
2.3.5 Institutionalized Information Assurance

Institutionalizing Information Assurance (IA) across the Marine Corps means that Marines and systems embody a sense and capability for valuing *information as a strategic asset*. It requires a total force approach to ensure that IA skill sets and proficiencies are codified and ingrained through doctrine, policy, education, and training. IA ensures the confidentiality, integrity, availability, authenticity, and non-repudiation of enterprise information and the information system on which the information resides. By continuing to professionalize the IA workforce the Marine Corps can better leverage enterprise information to help negotiate and succeed in a dynamic security environment. Additionally, the Marine Corps will continue to use existing development processes and continue to refine certification and accreditation processes to ensure IA requirements are identified and included early in a systems design project. Continual refinement and incorporation of emerging policies and guidance from the IA and acquisitions communities will better ensure IA controls are inherent to the system, thus providing superior and transparent threat protection across a wide range of missions.

3 STRATEGIC CONTEXT

3.1 THE CHANGING CHARACTER OF CONFLICT

The complex and changing character of conflict in the 21st Century is a critical factor affecting how Marines and their mission partners will use information and technology to achieve mission success. Emphasizing this point, the Marine Functional Concept for Command and Control notes that “US military preeminence in traditional forms of warfare has driven our adversaries to pursue combinations of conventional and irregular warfare, cyber-warfare, terrorism, and criminality to further their aims.” Going an additional step, Marine Corps Vision & Strategy 2025 explains that these methods and types of conflict will comprise a complex pattern of conventional, irregular, and hybrid challenges that can be created by states, proxy forces, non-state actors, or cyber groups. In addition to this complex array of challenges, US security strategy emphasizes the need for those activities that prevent conflict (e.g., security cooperation, building partner capacity, humanitarian assistance, and train, advise, assist activities). In sum, the scope, breadth, frequency, and pace of military operations in the 21st Century far exceeds our past experiences. Figure 5, derived from the Functional Concept for Command and Control, illustrates changes in the character and conduct of military operations.



New Operating Challenges

Threat
Traditional
Irregular
Catastrophic
Disruptive

Role of Military
Combat
Security
Engagement
Relief & Reconstruction

Scenario
US-led
Mostly Coalition
Coalition, Interagency
Homeland Defense

Changing Characteristics & Conduct of Military Operations

20th Century	21st Century
Massed Force	Dispersed Force
Information Based	Knowledge Based
Reactive	Proactive
US Military Centric	Interagency, Multinational
De-conflicted Operations	Integrated Joint Operations
Intermittent Pressure	Continuous Pressure
Bn Level Sustained Operations	Co Level Sustained Operations

Figure 6. Changing Characteristics and Conduct of Military Operations

The principal distinguishing characteristic of the 21st Century operational environment is the degree to which information and knowledge, as strategic assets, influence the characteristics and capabilities listed on the right side of Figure 6. While information and knowledge have always been decisive in military operations, the degree to which we will depend on these resources for competitive advantage will increase for the foreseeable future. This compels the need for us to consider the Marine Corps, in total, as an *Information Enterprise* – in a way similar to how we think of the Corps’ warfighting structure as the Marine Air Ground Task Force (MAGTF). **Because information and knowledge are as important for our success as it is for our adversaries’ potential for challenging our success, balancing investments in people, processes, information, and technology is critical to achieving sustained decision and execution superiority.**

3.2 THE PHYSICAL DOMAIN

The MCIENT exists across several domains, including the physical domain. This domain represents the tangible three dimensional space, plus time, where we physically move and operate. From an operational perspective the physical domain includes the terrain, weather, enemy and friendly formations, and the systems necessary for conducting military operations. **The MCITE and the MCEN comprise complex communications and information technology (IT) systems, within the physical domain, that facilitate the flow of information across the Marine Corps.**

3.3 THE INFORMATION ENVIRONMENT

The Department of Defense (DOD) defines the *Information Environment* as the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." (JP 1-02, DOD Dictionary of Military Associated Terms, 2009). According to recent DOD research, information is considered distinct from data because it provides context and meaning for action. Similarly, knowledge is distinct from information because it enables action directly (Nissen, 2006, p.12). Furthermore, knowledge generally exists in two forms: *explicit* and *tacit*.

Explicit knowledge can be characterized best as that which can be "articulated through words, diagrams, formulae, computer programs, and like means." Standing in contrast with this definition is *tacit* knowledge, which can be characterized as that which cannot be or has not been articulated (Nissen, 2006, p. 247). This vision and strategy document recognizes these important distinctions and definitions because they greatly affect how information and knowledge should be managed within the MCIE in the future. This document also recommends the Joint definition for information and knowledge be updated to reflect these important distinctions. Such distinctions would significantly help to advance IM and KM institutionally.

To fulfill this document's purpose, the term *Information Environment* is generalized to include data, information, and explicit knowledge because they can be readily communicated by physical means such as technology and communications systems. At the heart of the MCIE is the MCEN and those associated technology systems, organizations, and people that create, communicate, and use the information environment to facilitate command and control (C2) and mission planning and execution. However, in keeping with the definition of tacit knowledge, we recognize that communication within the information environment does not always depend upon technology solutions (e.g., implicit communications, shared experiences etc.). **By facilitating the integration of information, systems, people, and processes, the MCIE exists as a broad domain for facilitating the flow of information and knowledge across the Marine Corps and with mission partners.**

3.4 CYBERSPACE

The Department of Defense (DOD) defines Cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" (JP 1-02, DOD Dictionary of Military Associated Terms, 2009). Cyberspace therefore transcends both the physical domain and the information environment. The MCEN, MCITE, and MCIE all exist within Cyberspace. The Marine Corps Cyberspace Concept calls for improved capabilities to operate within this domain:

> The ability to operate in the cyber domain with the same skill as on land, sea, or air is critical to the Marine Corps' future operational success. Without mastery of computerized technology, many weapon and C2 systems will not work; Intelligence, Surveillance, and Reconnaissance will be ineffective; and sensitive information will be at risk of compromise. Adversaries recognize that much of the United States' economic and military dominance is heavily tied to technology, communications, and automated systems that are enabled by Cyberspace and they constantly seek to get a competitive advantage within this domain. (Marine Corps Cyberspace Concept)

The MCIENT enables USMC cyberspace operations by providing the necessary assets, organizations, processes, and personnel for performing some cyber disciplines (NetOps, IA, CNO). **The MCEN, MCITE, and MCIE represent the principle components to which Cyberspace operations apply.**

3.5 THE COGNITIVE DOMAIN

The cognitive domain is distinct from the information or cyber domains because it represents the non-tangible "space" within the human mind where *tacit knowledge* exists. Examples of mission critical tacit knowledge include human perception, shared human experiences, culture, awareness, understanding, beliefs, and values. For military operations that require support of the civilian population, such as counterinsurgency (COIN) operations, the military force that can grow organizational tacit knowledge will more likely succeed. Figure 6 supports this notion by identifying the need to develop a *Knowledge-based Force* to ensure we maintain a competitive edge over our adversaries. **While the MCIE is limited in its ability to directly transmit or represent tacit knowledge, it does communicate crucial data, information, and explicit knowledge that often provide the necessary context for building awareness and understanding in the cognitive domain.**

3.6 THE HUMAN SOCIAL NETWORK

The human social network represents another important factor of the strategic environment. This network is unique because it facilitates the flow of both tacit knowledge, and the flow of data, information, and explicit knowledge. Through the human social network, people or groups of people communicate slow-to-develop tacit knowledge through shared human experiences such as culture, tradition, and custom. The human social network also facilitates the communication of data, information, and explicit knowledge by leveraging traditional means of communication (e.g., communications systems, information technology, verbal communications, written word, etc.). For military operations that require support of the civilian population, such as COIN operations, the military force that can leverage both tacit and explicit forms of knowledge within the human social network will more likely succeed. **The MCIE represents a crucial capability that can help Marines and their mission partners harness data, information, and explicit and** t**acit knowledge flowing through the social network because it expands the reach of data, information, knowledge, systems, and people.**

3.7 THE THREAT ENVIRONMENT

MCIENT components exist within a constantly evolving logical and physical threat environment and may be the target of individual or combined and coordinated attacks. Because an information advantage is often strategically decisive, we must protect the MCIENT's components from attack or disruption. This vision and strategy document asserts that we must always assume our information capabilities and communications systems are under attack or at risk of disruption from both internal and external threats. Internal threats include intentional and unintentional activities from users that degrade or disrupt information and communications systems. External threats include computer hackers (e.g., state or non state sponsored, etc.) and natural disasters. A robust information assurance (IA) capability combined with sound Operations Security (OPSEC), Continuity of Operations Planning (COOP), and extensive training and education is essential to ensuring we maintain our Corps' freedom of maneuver through an uncertain security environment. **MCIENT components, organizations, people, and processes must be organized, equipped, trained, and governed from a perspective that always assumes our information capabilities are at risk while at the same time ensuring these capabilities are made available to Marines and authorized mission partners whenever and wherever they are needed.**

4 MCIENT OBJECTIVES AND RESOURCES

FOCUSED ON DEPLOYED FORCES

4.1 STRATEGIC OBJECTIVE 1: ENHANCE OUR ROBUST, SEAMLESS, AND SECURE MCEN

A robust, seamless, and secure Marine Corps Enterprise Network (MCEN) is at the root of Marine Corps communications and the MCIENT. We must enhance our MCEN to better serve deployed forces by improving seamlessness, reachback, interoperability, and security.

Strategic Objective 1 Resources

4.1.1 ADCON, TACON, and OPCON of the MCEN

To ensure our enterprise network continues to effectively support Marines and their mission partners in the operational environment, the Marine Corps must maintain Administrative Control (ADCON) and Tactical Control (TACON) of MCEN infrastructure and network services. Additionally, through MARFORCYBER, the Marine Corps must communicate and coordinate Service requirements for Operational Control (OPCON) of the MCEN with US Cyber Command (USCYBERCOM) to ensure the Marine Corps can operate as a Marine Air Ground Task Force (MAGTF) in support of a Joint Task Force (JTF), Allied, or in support of Marine Corps specific missions. Retaining control of the MCEN will ensure the Marine Corps remains a global expeditionary force capable of transiting seamlessly through multiple Combatant Commander (COCOM) areas of operation and operating in dispersed austere environments. Moreover, it will allow for the distribution of data, applications, and services closer to deployed Marines. **The MCEN is a core asset and capability that enables the Marine Corps to fulfill its role as the Nation's expeditionary force in readiness. Preserving the MCEN's integrity through effective ADCON, TACON, and OPCON is crucial to leveraging and protecting data and information.**

4.1.2 Agile Networking

To better support our deployed Marines we must develop and employ self forming, self healing, and mobile ad-hoc networks that deliver on demand access to data, applications, computing, and C2 services. These agile network characteristics are crucial for enhancing our ability to provide continuous voice, video, and data services to Marines operating at any level of unit aggregation, disposition, or location while on-the-move (OTM) or at–the-halt (ATH). Additionally, agile networks permit the movement of terminal services to and from the celestial (i.e., satellite communications), aerial (e.g. airborne retransmission, etc.), and the terrestrial (e.g., line of sight, etc.) transmission segments.

4.1.3 Globally Connected and Interoperable Transport

Transport shall employ a flexible, reliable, secure, timely, and survivable infrastructure that incorporates global connectivity and interoperability of all Marine Corps legacy and future C2, hand held, man portable, and vehicular transmission, switching, and computing platforms. Transport provides the communications infrastructure that ties our bases, posts, and stations together and provides a means for our tactical forces to reachback into the Supporting Establishment. **Our transport architecture represents a potential critical vulnerability if this resource is not sufficiently planned and resourced. The Marine Corps will plan for continued improvement and modernization of transport capabilities such as: Tactical Communications Modernization (TCM), Warfighter Network Services – Tactical (WFNS-T), Base Telecommunications Infrastructure (BTI), and Enterprise Land Mobile Radio (E-LMR).**

4.1.4 Networking on-the-Move (NOTM)

NOTM is family of systems that promotes/supports an OTM terrestrial, celestial, and aerial network providing Beyond Line of Sight (BLOS) extensions using a combination of existing, planned, and new initiatives. This family of systems represents a modernization initiative that will fundamentally improve the speed, tempo, and reach of

Marine Forces operating in all environments. NOTM employs self forming, self healing, secure, mobile, and agile ad-hoc networks to permit the movement of Marines without loss of service. This modernization initiative improves the ability for dispersed or aggregated Marine Corps units to operate and communicate without pause. "The need for [communications] on the move will continue to increase as future operating environments will demand the application of military power in ever-smaller increments, which in turn will require the achievement of joint synergy at ever-lower echelons of command" (Capstone Concept for Joint Operations, 2009, p. 25).

To facilitate this capability the Marine Corps will develop, align, and deliver systems that are capable of providing a self-forming / healing ad-hoc mobile network to facilitate OTM communications, OTH, and beyond line of sight (BLOS) capability down to the Company level across the MAGTF. This network capability allows delivery of information critical to the planning process and allows commanders to control networking assets. NOTM enables mobile forces to collaborate and access information resources (e.g., databases, collectors, etc.) to exchange voice, data, and video information. It provides crucial network management capabilities to simplify the planning, configuring, and monitoring of the MAGTF's OTM network. This system will connect to ATH digital backbone long haul communications architectures that comprise the MCEN and the GIG. (MAGTF Requirements List, NOTM Concept of Employment)

4.1.5 Network Enabled Radios

The Marine Corps will deploy Internet Protocol (IP) routable/data-capable radios that are vehicular/aircraft mounted and/or man portable (e.g., hand held devices, etc.) that will integrate data and voice capability into one radio transmitter. These radios are a NOTM extension providing C2 capability to the lowest echelon of our combat elements. These radios will be part of a self forming, self healing, ad-hoc network.

4.1.6 Information Assurance

The Marine Corps will institutionalize IA as a core practice to better ensure we can leverage communications and IT systems modernization. Information Assurance (IA) provides a critical capability for enhancing our robust, seamless, and interoperable MCEN. IA policy and practice must allow Marines to interoperate with external networks (e.g., Joint, Allied, Coalition, etc.) to facilitate seamless information sharing. Additionally, IA policy and practice must enable Marines to evaluate and rapidly implement emerging technologies and software applications. Finally, the Marine Corps will comply with all IA workforce training, certification, and education policies to ensure that Marine Corps communications and IT systems operate with the requisite level of confidentiality, integrity, availability, authenticity, and non-repudiation.

4.1.7 Information Exchange Standards

The Marine Corps will implement low and high bandwidth net-centric data and information exchange standards for mission partner interoperability. The DOD is partnering with other government agencies to improve information sharing by implementing high-bandwidth net-centric standards such as Universal Core and Command and Control Core Community of Interest (COI) vocabularies. The increasing availability of high-bandwidth, reliable communication networks is enabling the DOD to migrate to these more efficient, more flexible data exchange standards in the deployed environment. The ability of operating forces to prioritize their information requirements is necessary for supporting users when data and information loads exceed available bandwidth.

However, the Marine Corps anticipates that technical message standards, such as Variable Message Format (VMF) and Tactical Data Links will continue to be required to support Disconnected, Intermittent, and Low-bandwidth (DIL) users. The Marine Corps also understands that in a fiscally constrained environment new initiatives for developing information exchange assets may be limited; therefore it is imperative that current standards be maintained. The Marine Corps will continue to advocate master data management and data standards (e.g., MIL-STD 2525, etc.) as the principle basis for achieving mission partner interoperability. By leveraging standards, the Marine Corps will fulfill its requirement for interoperability while at the same time retaining ADCON, TACON, and OPCON of the MCEN.

The Marine Corps supports the concept for interoperability as defined in the Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD): "Standards provide effective enterprise direction for data standards, information service standards, acquisition, certification, and enforcement to ensure seamless flow of information between all DOD and mission partner users and systems."

4.2 STRATEGIC OBJECTIVE 2: IMPROVE REACHBACK SUPPORT AND INTEROPERABILITY

The Marine Corps will enhance our MCEN by improving reachback support and interoperability of our forward deployed forces. An effective reach-back communication system enables the Commander to conduct dispersed operations in a non-linear battlespace by providing more information with fewer deployed forces, by providing connectivity to adjacent forces over greater distances, by providing visibility to higher headquarters, and by allowing for more assets to be brought to the situation as needed. The net-centric information environment also provides battalion and below forces with access to rear echelon data resources. The communications system must be interoperable, agile, trusted, and shared - leveraging non organic capabilities inherent in other organizations.

Strategic Objective 2 Resources

4.2.1 Forward Deployed Data, Information, and Knowledge

The Marine Corps concept for forward deployed data, information, and knowledge is rooted in the assumption that forward deployed Marine Forces will continue to operate with severe network degradation, throughput and bandwidth constraints. This assumption forces the Marine Corps to broadly distinguish the need for forward deploying data, information, and knowledge from a cloud computing concept where deployed forces access the "cloud" for needed resources. Because cloud computing, as a generic concept, requires data communications for remote data access, the Marine Corps cannot accept the risk of depending upon cloud computing concepts for forward deployed forces. The Marine Corps will seek to use cloud computing concepts and virtualization technologies where sensible, including perhaps, among its garrisoned forces and supporting establishment.

4.2.2 IT Regionalization

Marine Corps IT regionalization distributes IT services across the Marine Corps to support enterprise, regional, and local users. This concept enhances reachback support and interoperability by providing access to IT services closer to deployed forces. Additionally, regionalization allows regional and local commanders maximum network flexibility and responsiveness to COCOM operational requirements. Regionalization balances centralized management and regionalized management to support all organizations that depend on the MCEN for mission execution. This regionalization concept provides the physical and governance mechanism for retaining ADCON, TACON, and OPCON of the MCEN. It also improves the security of our enterprise network by employing a robust defense-in-depth IA posture.

4.2.3 Community of Interest Network (COI-NET)

To enhance reachback support and interoperability, the Marine Corps will establish a scalable, secure, gateway that facilitates access to communities of interest (COIs), communities of practice (COPs), Subject Matter Expert networks (SME-NETs), Social Networking Sites (SNSs), and other information necessary for collaboration. For example, operational forces could establish a COI NET with the Supporting Establishment, government agencies, NGOs, joint and multinational mission partners, industry, and field service representatives to enable access to a common interface for collaboration in support of training, education, planning, and operations.

4.2.4 "Plug and Play" Transport Connectivity

Reachback and interoperability are provided by celestial (satellite), aerial (airborne relay), and terrestrial (line of sight (LOS)) communications networks that facilitate access to higher, adjacent, and subordinate communications networks. The Computer Network Defense (CND) boundaries that connect to non-Marine communications networks need to be scalable and easily implemented as we gain access to or leave these adjacent networks at the lower echelons of ground combat, aviation combat, and logistics combat elements. Equipment, policies, and processes need to facilitate this “plug and play” concept for connectivity.

4.2.5 Joint, Inter-Agency, Multinational, and Non-governmental Interoperability Standards

The Marine Corps will influence the development of standards to enhance reachback support and interoperability. Standards allow disparate individuals, groups, and organizations with differing equipment and communications systems to exchange data and information securely and reliably. **Equipment, applications, and the development and implementation of policy and training must be based on common, multinational (e.g., International Standards Organization (ISO), open NATO Standard Agreements (STANAGS), etc.), and non-proprietary solutions.**

4.3 STRATEGIC OBJECTIVE 3: ENABLE MARINE CORPS COMMAND AND CONTROL

MCIENT components must be continually improved to support Marine Corps command and control (C2). For instance, the MCEN is central to the Marine Corps Functional Concept for Command and Control, where C2 is envisioned as leader-centric and network enabled, connecting all elements of the MAGTF with joint forces and mission partners to improve information sharing and collaboration. The concept will leverage a distributed network to improve unity of effort and speed of command by connecting organizations that can synchronize and integrate their force elements at the lowest levels.

Strategic Objective 3 Resources

4.3.1 Leader Centric Transport

Transport enables the Marine Corps Functional Concept for Command and Control by facilitating internal MAGTF elements to communicate with one another using terminal devices and applications. The transmission system architecture will provide a dynamic, decentralized, distributed, and highly adaptive communications network that enables C2. Leader-centric C2 that is network enabled requires a highly adaptive transport layer that enables a leader-centric information flow. These transmission devices must be self-forming, self-healing, mobile, ad-hoc, secure, easily configurable, and expeditionary in nature.

4.3.2 Application Hosting

The Marine Corps will leverage MCEITS, as well as GIG services, to support the Marine Corps Functional Concept for Command and Control. MCEITS is a core capability within the Marine Air Ground Task Force Command and Control (MAGTF C2) Framework and System of Systems (SoS). MCEITS contributes to the MAGTF C2 Framework end-to-end capability by enabling access to enterprise information and by providing the ability to collaborate and share information across the warfighting and business domains. MCEITS accomplishes this by implementing an IT infrastructure with application, services, and data environments. MCEITS must quickly and easily adapt to evolving software, hardware, data, services, and management requirements while providing enhanced enterprise visibility that facilitates greater reuse of its assets. MCEITS and other components (e.g., Marine Corps Intelligence Surveillance and Reconnaissance Enterprise (MCISR-E)) must provide responsive support for a secure, collaborative, interoperable data sharing environment while enabling the integration of products, services, and users via a service-oriented architecture (SOA). These capabilities support and contribute to the DOD’s overall GIG enterprise services (GES) and net-centric enterprise services (NCES).

4.3.3 Marine Corps Intelligence, Surveillance and Reconnaissance Enterprise (MCISR-E)

The Director Marine Corps Intelligence (Director I) will continue establishing a database structure that integrates all Marine Corps intelligence disciplines (e.g., Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), and Signals Intelligence (SIGINT)). This structure will emphasize enterprise commonality requirements and facilitate interoperability with other USMC functional disciplines (e.g., C2, Logistics, Aviation, etc.) whenever applicable. It will include multinational formats and protocols for interoperability with Allied and Coalition mission partners. This common data structure will support efficient sharing of classified information up to Secret via gateways between Top Secret networks and USMC Intelligence and other functional disciplines in accordance with security policies.

4.3.4 Data Availability and Recovery

Data is central to enabling command and control (C2). Ensuring data availability for C2 is a core function of IT Regionalization and MCEITS. To ensure data remains available during periods of disruption it is essential to develop and employ robust and viable High Availability / Disaster Recovery (HA/DR) plans regionally and for the enterprise. HA/DR is a key performance parameter of MCEITS. In order to achieve HA/DR at an enterprise level, policy directing the migration of services and data to MCEITS is important for achieving this objective.

4.4 STRATEGIC OBJECTIVE 4: INFLUENCE AND INFUSE EMERGING TECHNOLOGIES

To ensure Marines and their mission partners are sufficiently equipped to succeed in an uncertain security environment, the Marine Corps must develop innovative ways to influence and infuse emerging commercial and government-developed technologies. The rate of technological innovation and change far exceeds Government-mandated development and acquisition processes.

Strategic Objective 4 Resources

4.4.1 IT Acquisition Reform Advocacy and Leveraging Inherent Skills and Innovation

While remaining compliant with DODI 5000.02 requirements, the Marine Corps will work with the Office of the Secretary of Defense (OSD), Joint Chiefs of Staff (JCS), the Department of the Navy (DON), and our sister Services to advocate for IT acquisition legal reform. Additionally, the Marine Corps will seek better ways for bringing technologies to bear by using inherent skills and talent across the organization. For example, the Marine Corps should implement and incentivize an inherent capability for quickly and securely creating and fielding software applications for server, desktop/laptop, and mobile computing devices by using programming talent resident within the Marine Corps. Achieving this would require instituting an approved secure software development toolkit that is made widely available to forward deployed or garrison based Marines, Civilian Marines, and support contractors.

4.4.2 Force Development Roles and Responsibilities

The Director C4 / DDCIO (MC) will coordinate with Deputy Commandants, Directors, Marine Corps Systems Command, Marine Forces (MARFORs), and other agencies within the Supporting Establishment (SE) to review and refine organizational roles, responsibilities, and products necessary for participating in the Force Development process. The Director C4 / DDCIO (MC) currently provides IT Steering Group evaluation results to inform the programming priorities. The Director C4 / DDCIO (MC) also provides the enterprise objectives listed in this strategy to inform senior leader Force Development guidance.

ATTUNED TO THE STRATEGIC ENVIRONMENT

4.5 STRATEGIC OBJECTIVE 5: ASSESS, REACT TO, AND INFLUENCE THE STRATEGIC ENVIRONMENT

A MCIENT that is attuned to the strategic environment enables the Marine Corps to achieve competitive advantage by enabling Marines to better assess, adapt to, and influence changes in the strategic environment. This objective is particularly focused on the MCEN and MCITE as they are often our adversaries' focus of cyber-attack. Because information and knowledge are strategic assets impacting all military missions and activities across the range of military operations, the ability to assess, react to, and influence the strategic environment depends on our ability to leverage a flexible network that helps us anticipate, defeat, and mitigate threats to the data, information, and knowledge our Marines and mission partners need.

Strategic Objective 5 Resources

4.5.1 Enterprise Tools, Policy, and Process

Enterprise tools help Marines assess threats and challenges to the MCIE as well as assess the current state of the MCIE. Enterprise tools are used to implement directives and policies from higher headquarters, as well as internal Marine Corps requirements. Enterprise policies help Marines react to or influence changes in the strategic environment that impact MCIENT components by directing Marines how and when to use tools that affect changes necessary to mitigate or defeat the assessed threat or challenge. Tools and policies are together implemented via processes (e.g., IT Service Management (ITSM), etc.) to provide a holistic capability for operating and defending MCIENT components. **The Marine Corps must retain control of MCIENT components, such as the MCEN, in order to operate in support of the Joint Task Force (JTF) or Marine Corps task organized missions.**

4.5.2 IT Service Management (ITSM)

The Marine Corps will establish an ITSM framework through which NetOps (IT Operations) will be achieved and maintained, 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, cross-organization cooperation, and participation and leadership from the Marine Corps' IT service strategy community. Figure 3 depicts NetOps and ITSM in relation to other MCIENT components and institutional organizations, processes, and personnel.

4.5.3 Flexible Network

In order to conduct high tempo operations with resilient and reliable communications that assure access to the information environment, we must employ and operate a *flexible network* that can adjust rapidly and dynamically to counter external and internal degradation and mission changes. Employing and operating such a communications network requires a well designed and engineered architecture, continual assessment of the strategic environment, sufficient tools and policies, regionalization of the MCEN infrastructure, and a well trained workforce. These dependencies frame the requirement for the Corps to maintain a decentralized communications network that enables institutional flexibility.

4.5.4 Cyberspace Intelligence

Intelligence helps the commander assess the strategic environment by providing tailored products and assessments that improve awareness, understanding, and decision making. Within Cyberspace, intelligence regarding the cyber threat to MCIENT components is of strategic consequence. The Marine Corps must leverage superior intelligence to forecast threats and rapidly mitigate and counter their effect on the enterprise. The Marine Corps must ensure intelligence is produced and used holistically to enhance our ability to conduct cyberspace operations. Cyberspace Intelligence must ensure a shared awareness of network health, network vulnerabilities, and emerging or imminent network threats. Additionally, Cyberspace Intelligence must incorporate and use tactical computer forensics to ensure a more complete picture of the threat environment.

GROUNDED IN EFFECTIVE GOVERNANCE

4.6 STRATEGIC OBJECTIVE 6: MAN, TRAIN, AND EQUIP THE FORCE FOR THE MCIENT

The Commandant of the Marine Corps is responsible for manning, training, and equipping the force for the MCIENT. The Director C4 is the Commandant's principal advisor for all Title 10 matters and responsibilities related to the Information Enterprise. The Director C4 will periodically review the organization and processes designed to support the execution of delegated Title 10 responsibilities.

Strategic Objective 6 Resources

4.6.1 Director C4 Governance Organization

The Director C4 leverages HQMC C4 organizational components to produce the products and policies necessary for informing Force Development guidance and priorities. The Director C4 plans, directs, and coordinates all staff activities relating to C4 functions, and supports the Commandant in his role as a member of the Joint Chiefs of Staff. In addition, the Director C4 serves as the Marine Corps CIO and the Deputy Commanding General for MARFORCYBER. In this capacity, the Director C4 is responsible for managing IT as a Marine Corps strategic asset.

4.6.2 Director C4 Governance Process

The Director C4 leverages institutionalized processes to develop, operate, and manage MCIENT components. The Marine Corps participates in and informs the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management Framework (i.e., Joint Capabilities Integration and Development System (JCIDS); Defense Acquisition System (DAS); and the Planning, Programming, Budgeting, and Execution (PPB&E) process). The Marine Corps also employs several DOD, DON, and Marine Corps specific processes in conjunction with the above processes to develop, acquire, and operate MCIENT components (e.g., Advocacy, Expeditionary Force Development System (EFDS), Defense Information Technology Information Library (DITIL), and Enterprise Information Technology Services Management (E-ITSM)). **In order to ensure the MCIENT effectively supports evolving Marine Corps requirements, the Director C4 must periodically review applicable processes to ensure they align they support governance requirements.**

4.6.3 "Network Marine" Training

Communications training must be focused on creating a "Network Marine" who understands and is able to execute his or her greatest potential in supporting the Network. Trained beyond the simple operation of a piece of equipment, the Network Marine must understand the capabilities of the MCEN as it relates to the other MCIENT core components, and have the expertise and empowerment to exercise appropriate initiative in coordination with communications control to restore, reinforce, and strengthen network capability. In order to achieve this goal, the USMC Communications Military Occupational Specialty (MOS) structure and training establishment must transition from the infrequent training opportunities to constant, continuous, and real time training that keeps the Network Marine abreast of dynamic changes in MAGTF communications architecture.

4.7 STRATEGIC OBJECTIVE 7: EXECUTE CIO RESPONSIBILITIES AND CORE COMPETENCIES

A body of Federal law and policy (e.g., Clinger Cohen Act, OMB Circulars, etc.) establishes the requirement for federal agencies and military organizations to have a Chief Information Officer. This body of law also governs the responsibilities and activities of CIOs. The DDCIO (MC) performs the responsibilities and activities that are necessary for ensuring Marine Corps compliance with standards and policies for ensuring IT and workforce strategies, architectures, and investments efficiently achieve organizational requirements. The MCIENT model provides an organizing framework to assist the DDCIO (MC) in performing CIO duties.

Strategic Objective 7 Resources

4.7.1 CIO Organization

The organizational structure used to support the DDCIO (MC) exists within HQMC C4. The Marine Corps will periodically review the DDCIO (MC) support structure to ensure it can effectively assist the CIO's ability to perform applicable responsibilities and activities established in law and policy.

4.7.2 CIO Functions and Processes

Through the organization, the DDCIO (MC) leverages standardized processes to execute inherent responsibilities and activities (e.g., Capital Planning and Investment Cycle (CPIC), Portfolio Management, Enterprise Architecture, Annual Reviews, and Systems Registration, etc.) to ensure the Marine Corps achieves required capabilities with cost effective solutions, and to ensure the Marine Corps complies with required laws, policies, and federal mandates (e.g., Clinger Cohen, Green IT mandates, etc.). The Marine Corps will periodically review applicable CIO processes, such as the IT Steering Group (ITSG) to ensure they align to federal law and higher level policy and processes within DOD and DON.

4.8 STRATEGIC OBJECTIVE 8: INSTITUTIONALIZE STRATEGIC PLANNING AND LIFECYCLE MANAGEMENT

The Marine Corps will establish a standardized MCIENT Strategy Development and Lifecycle Management Process as depicted in Figure 1. The process is designed to provide the Director C4 / DDCIO (MC) with a continuous and structured method for coordinating the development of enterprise objectives that achieve the MCIENT vision and inform Force Development investment priorities. Furthermore, the Strategy Development and Lifecycle Management Process will ensure the MCIENT Strategy is: (1) *developed* in support of Marine Corps objectives, (2) *communicated* across the Corps and to external audiences, (3) *executed* by the organization, and (4) is *assessed* and *reviewed* for relevance and for vision/mission accomplishment.

Strategic Objective 8 Resources

4.8.1 MCIENT Strategic Planning Group

Under flag level leadership, the Director C4 / DDCIO (MC) will establish and direct the efforts of a Strategic Planning Group (SPG) responsible for executing and coordinating all activities and products required by the MCIENT Strategy Development and Lifecycle Management Process. The DDCIO (MC) shall charter this group to provide the strategic direction necessary to ensure MCIENT capabilities, plans, and policies are useful to the Force Development process. As a function of its charter, the group shall coordinate with MCIENT implementation stakeholders such as the Operational Forces (OPFOR), USMC Deputy Commandants, Directors, Marine Corps Systems Command, and others to capture functional requirements and translate them into Information Enterprise objectives that inform CMC or MROC Force Development guidance. Additionally, the group shall collaborate with USMC, joint, interagency, academic, and industry or government visionary organizations to stay abreast of changes in the strategic landscape, cutting edge technologies and concepts, and non-material solutions. Members of this group shall comprise subject matter experts that can coordinate with all the above organizations or agencies and who are skilled in the art and process of strategic assessments and planning.

4.8.2 MCIENT Strategic Planning and Lifecycle Management Process

The MCIENT Strategic Planning and Execution Process is a four step process (indicated in Figure 3) that includes *strategy development*, *strategy communication*, *strategy execution*, and *strategy assessment and review*. The SPG executes this process.

DELIVER A SECURE AND SEAMLESS INFORMATION ENVIRONMENT

4.9 STRATEGIC OBJECTIVE 9: IMPLEMENT A FEDERATED DATA ENVIRONMENT

Federating data across the MCIENT is central to delivering a robust and seamless information environment. Data federation means that structured and unstructured data (e.g., databases, imagery, audio, etc.) is distributed across the information environment in a series of interrelated and linked authoritative data sources. Federation is crucial to implementing a robust defense-in-depth IA strategy because it decentralizes and replicates data services to protect enterprise segments from data loss during periods of disruption. Additionally, the Marine Corps will participate in the development of multinational standards (e.g., STANAG 4609, etc.) and publish adopted standards to facilitate mission partner interoperability.

Strategic Objective 9 Resources

4.9.1 Data Advocacy

The Director C4 / DDCIO (MC) will coordinate with the Office of the Secretary of Defense (OSD), Joint Chiefs of Staff (JCS), the DON, our sister Services, Deputy Commandants (DCs), Director Intel (Dir I), and Marine Corps Systems Command (MCSC), and any other organization involved in the planning, development, operation, or governance of MCIENT components to define the implementations required for ensuring data is visible, accessible, discoverable, and understandable in a way consistent with Marine Corps needs. The Marine Corps must assume a financially constrained future and must therefore achieve efficiencies through common enterprise data solutions where sensible.

4.9.2 Data Policy

The Dir C4 / DDCIO (MC) will provide guidance that supports DOD and DON mandates to enhance our ability to share and integrate data and improves data management and administration practices in order to ensure data quality meets or exceeds mission needs. This guidance will support the exchange of timely and relevant data and information by elaborating on data advertisement and discovery; data access, protection, and storage; and data replication, linking, and federation.

The Marine Corps has data policy requirements for tagging new structured and unstructured data created by data producers (e.g., people, sensors, processes, systems, and applications, etc.). The policy also reflects the requirement to get data from authoritative data sources and leverage information exchange standards. Data provenance requirements reflected in policy will be addressed by tagging data and information with metadata containing classification markings, disclosure, reliability, and handling rules.

4.10 STRATEGIC OBJECTIVE 10: IMPLEMENT DISTRIBUTED SERVICES

The Marine Corps will distribute enterprise services regionally and to forward deployed forces in order to facilitate the delivery of a robust and seamless information environment. Distributing services is a central tenant of the net centric force. Achieving this goal will enhance Marine Corps organizational and tactical agility and flexibility, as well as improve information sharing across the total force.

Strategic Objective 10 Resources

4.10.1 MCEITS

The MCEITS program provides a standard infrastructure to distribute enterprise data and cloud services regionally and to forward deployed forces when feasible. MCEITS improves IT cost efficiencies by providing centralized data services federated under the DoD Information Enterprise. Additionally, MCEITS provides high availability, disaster recovery, and continuity (HA/DR/C) for enterprise applications. MCEITS represents a critical capability for achieving streamlined and consolidated enterprise portfolios that reduce total cost of enterprise ownership by reducing our requirement to maintain expensive legacy enterprise applications. In a financially constrained environment it is imperative that the Marine Corps take advantage of MCEITS to lower the total cost of owning data applications.

4.10.2 IT Regionalization

IT regionalization provides a governance mechanism for distributing services across the Marine Corps to support enterprise, regional, and local users operating principally within the garrison environment. This ensures regional network and information services management and expertise is available to support any Marine unit within the region. IT Regionalization is crucial to forward deploying data to Marines and their mission partners.

4.10.3 Tactical Distribution

The Marine Corps requires near-real-time, cross domain, and multi-level secure data distribution at the lowest tactical level to enhance joint, interagency, and multinational interoperability, as well as mission performance and force protection. Because this capability does not currently exist, the Marine Corps must invest in many-to-many data exchange capabilities with the above characteristics. For example, no solution currently exists for transporting or replicating bad actor data in near real time to or among Marine Corps units and joint or multinational mission partners operating in the field. Marines and their mission partners manning checkpoints should have near real time access to bad actor data, regardless of the data's authoritative production source.

4.11 STRATEGIC OBJECTIVE 11: IMPLEMENT A FEDERATED ENTERPRISE ARCHITECTURE

The Director C4 / DDCIO (MC) will lead the implementation of a federated Enterprise Architecture (EA) in order to establish an integrated EA view of Marine Corps segment architectures (e.g., Battlespace Awareness, Force Application, etc.). This integrated view will facilitate the alignment of USMC resources and capabilities to better execute core and joint missions and to inform the Force Development process. Marine Corps EA will be federated with DOD, DON, and the Intelligence Community (IC) Enterprise Architectures in order to eliminate Department redundancies where appropriate.

Strategic Objective 11 Resources

4.11.1 Enterprise Architecture Policy

The Marine Corps' EA will continue to comply with federal mandates and will federate with DOD, DON, and Intelligence Community (IC) level EA efforts. HQMC C4 shall continue to provide policy guidance and governance on architecture matters across the Marine Corps. This oversight serves to evolve and align EA content and enhance its usability. The architecture itself and its segment architecture products shall be developed using authoritative reference architectures, components, and frameworks compatible with the Joint, DOD, and Service architectures (e.g., Department of Defense Architecture Framework (DODAF)).

4.11.2 Enterprise Architecture Lexicon

The Marine Corps shall develop and publish a single authoritative EA lexicon consistent with the JCA lexicon and DOD EA definitions in order to facilitate the consistent and compatible development of segment architectures (e.g., Battlespace Awareness, Force Application, etc.). Director C4 / DDCIO (MC) will lead the development of this authoritative EA lexicon that will be made available to components developing architectures. This lexicon will inform organizations in the Marine Corps that produce requirements, develop capabilities, procure systems, manage portfolios, and manage programs of record during their respective acquisition lifecycle and related processes.

INSTITUTIONALIZE INFORMATION ASSURANCE

4.12 STRATEGIC OBJECTIVE 12: IMPROVE IA PROFICIENCY ACROSS THE CORPS

The Marine Corps will continue to improve the technical proficiency of the IA workforce, as well as IA awareness and training for all Marines to better protect our information and ensure mission success. In the same manner that Marines are trained in immediate action drills for use during patrolling or convoy operations, Marines need to understand what actions they should take when encountering a threat or attack (e.g., countermeasure employment and incident reporting).

Strategic Objective 12 Resources

4.12.1 Information Assurance Doctrine

The Marine Corps will develop IA doctrine consistent with Marine Corps maneuver warfare doctrine, enhanced company operations concepts, network centric theory, and scale free networks theory. Establishing doctrine represents a crucial first step toward IA institutionalization. IA, if properly institutionalized will better enable Marine Forces to maneuver in both the physical and information environments. It will establish the basis for developing future IA policies, education and training plans, procurement initiatives, architectures, and workforce requirements.

4.12.2 Information Assurance Policy

The Marine Corps will continue to develop IA policies that balance capabilities and risk with smart and secure enterprise operations while providing Marines the freedom of action to carry out their mission. Recognizing that much of IA is institutionalized across the DOD to enable joint operations and leverage the GIG, Marine Corps specific policies must support DOD policy while allowing the Marine Corps to retain ADCON and TACON of the MCEN. Our policies must be standardized throughout the Marine Corps and have quantifiable and verifiable criteria from which a holistic and dynamic security posture can be determined.

4.12.3 Information Assurance Training and Education

The Marine Corps will improve IA training and education by establishing a comprehensive plan that focuses on training and educating both the IA workforce and all others who use MCIENT components. IA training and education must be comprehensive and reinforced throughout a person’s career. It must be tailored to a specific audience and emphasize how the MCIENT operates and supports mission accomplishment as well as the common dangers associated with computing activities. Subsequent training should be targeted to the user’s billet and level of responsibility. The IA workforce needs to leverage *lessons learned* in order to capture and communicate best practices, hard-earned knowledge, and unique solutions to tough problems. Additionally, the Marine Corps will encourage IA workforce members and others with IA interest to pursue additional education and industry certifications to better ensure the Marine Corps improves its ability to creatively solve new IA problems and develop innovative solutions. Graduate level education opportunities should be made available to our Marines and Civilian workforce as they pursue voluntary professional IA development. Finally, the Marine Corps will better leverage academia and industry in its pursuit of ensuring a secure, operationally responsive MCIENT within the evolving security environment.

4.12.4 Information Assurance Workforce

The IA workforce in the Marine Corps includes Marines, Civilian Marines, and contracted IA professionals. The Marine Corps must continue to make investments in its IA workforce and ensure that the workforce is properly sized and trained in order to provide the appropriate level of enterprise security and operational flexibility. As new technology develops, related threats and responses will similarly develop. The IA workforce must be responsive to emerging threats and must continually reassess its posture to best protect and defend the enterprise. Today’s skills may be obsolete tomorrow with the advent of new hacker tools. Therefore, the workforce needs to be engaged in a comprehensive understanding of emerging threats and associated mitigations through continual education and self study. It is essential that the workforce is well grounded in IA and networking fundamentals so they understand not only how threats work but why they work. The IA workforce, armed with this breadth and depth of knowledge, can better advise and support commanders in the accomplishment of their missions while better protecting MCIENT components against an entire range of threats.

4.13 STRATEGIC OBJECTIVE 13: FIELD SYSTEMS WITH INHERENT IA CONTROLS

The Marine Corps will ensure that IA capability requirements are included in the systems design process as early as feasible. This will better ensure that systems (e.g., hardware, software, and middleware, etc.) are developed, procured, and fielded faster and with inherent IA controls.

Strategic Objective 13 Resources

4.13.1 IA Requirements

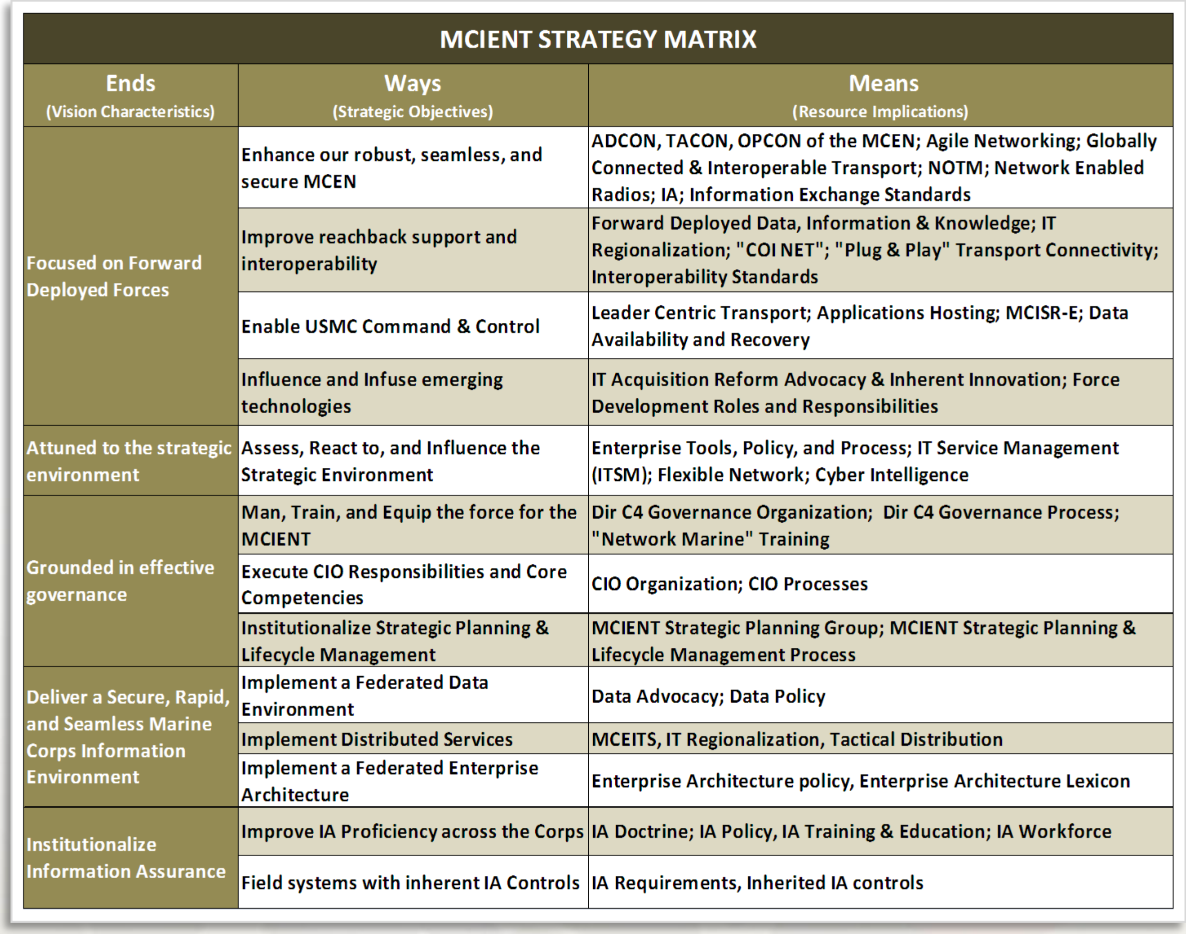
Integrating IA requirements early is critical to building self-forming, self healing, and ad-hoc networks because these networks require inherent IA controls that enhance a user's ability to dynamically and seamlessly transition through multiple networks. Inherent IA controls that are automatic, dynamic, and transparent to the user are central to achieving seamless network transitions. Additional benefits for including IA requirements early in the design process include reduced fielding and equipment modification costs, reduced system complexity, and reduced fielding time.

4.13.2 Inherited IA Controls

Inheritance is an important IA concept for the MCIENT and to rapid system fielding. This concept allows systems to use controls from related systems or sites in a parent – child relationship to partially fulfill IA control requirements. Inheritance provides efficiencies and more flexibility in the system design process by eliminating the number of controls the design team must build to, yet the system remains protected by the controls it inherits. The MCIENT's core components will provide a set of baseline controls that systems can inherit, thereby streamlining the system design process. These baseline controls will continue to evolve with the threat but will also continue to protect downstream systems residing in various states.

5 MCIENT STRATEGY MATRIX

The strategy matrix provides a useful and simple depiction of the vision and strategy by showing the specific alignment of Means and Ways to achieve Ends.



MCIENT STRATEGY MATRIX

Ends (Vision Characteristics)	Ways (Strategic Objectives)	Means (Resource Implications)
Focused on Forward Deployed Forces	Enhance our robust, seamless, and secure MCEN	ADCON, TACON, OPCON of the MCEN; Agile Networking; Globally Connected & Interoperable Transport; NOTM; Network Enabled Radios; IA; Information Exchange Standards
	Improve reachback support and interoperability	Forward Deployed Data, Information & Knowledge; IT Regionalization; "COI NET"; "Plug & Play" Transport Connectivity; Interoperability Standards
	Enable USMC Command & Control	Leader Centric Transport; Applications Hosting; MCISR-E; Data Availability and Recovery
	Influence and Infuse emerging technologies	IT Acquisition Reform Advocacy & Inherent Innovation; Force Development Roles and Responsibilities
Attuned to the strategic environment	Assess, React to, and Influence the Strategic Environment	Enterprise Tools, Policy, and Process; IT Service Management (ITSM); Flexible Network; Cyber Intelligence
Grounded in effective governance	Man, Train, and Equip the force for the MCIENT	Dir C4 Governance Organization; Dir C4 Governance Process; "Network Marine" Training
	Execute CIO Responsibilities and Core Competencies	CIO Organization; CIO Processes
	Institutionalize Strategic Planning & Lifecycle Management	MCIENT Strategic Planning Group; MCIENT Strategic Planning & Lifecycle Management Process
Deliver a Secure, Rapid, and Seamless Marine Corps Information Environment	Implement a Federated Data Environment	Data Advocacy; Data Policy
	Implement Distributed Services	MCEITS, IT Regionalization, Tactical Distribution
	Implement a Federated Enterprise Architecture	Enterprise Architecture policy, Enterprise Architecture Lexicon
Institutionalize Information Assurance	Improve IA Proficiency across the Corps	IA Doctrine; IA Policy, IA Training & Education; IA Workforce
	Field systems with inherent IA Controls	IA Requirements, Inherited IA controls

Figure 7. Marine Corps Information Enterprise (MCIENT) Strategy Matrix

6 GLOSSARY AND REFERENCES

6.1 GLOSSARY

Access - Opportunity to make use of an information system (IS) resource. (Committee on National Security Systems Instruction (CNSSI) No. 4009)

Administrative Control (ADCON) - 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 mission of the subordinate or other organizations. (JP- 1)

At-The-Halt (ATH) - a temporary pause in tactical operations. (DOD Dictionary, 2009)

Availability - Timely, reliable access to data and information services for authorized users. (CNSSI No. 4009)

Base Telecommunications Infrastructure (BTI) - The Marine Corps BTI initiative provides all Marine Corps installations with the communications infrastructure service that connects the end-user to the Defense Information Systems Agency (DISA) network. The ongoing focus is standardization on DISA Unified Capabilities (UC) (voice, video, collaboration, and data) through modernization of installation infrastructure in order to maintain connection to the DISA network. Marine Corps participation in the DISA UC Pilot will solidify the hardware and procedures to move voice into a Net-Centric environment. (BTI POM 12 Baseline Brief)

Capital Planning and Investment Control (CPIC) - A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes. (OMB Circular 130)

Certification (Individual) - Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval based on a set of standards for specific profession or occupations' functional job levels. Each certification is designed to stand on its own, and represents a certified individual's mastery of a particular set of knowledge and skills. (DODD 8570.1)

Network Certification - Comprehensive evaluation of the technical and nontechnical security safeguards (of a network) to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. (CNSSI No. 4009)

Chief Information Officer (CIO) - A position stipulated in the Clinger Cohen Act. CIO Duties include: (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with Chapter 35 of Title 44, United States Code, and the priorities established by the head of the executive agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency. (Clinger Cohen Act)

Clinger-Cohen Act (CCA) - The Information Technology Management Reform Act (ITMRA) (Division E) and the Federal Acquisition Reform Act (FARA) (Division D) were signed into law as part of the National Defense Authorization Act for Fiscal Year 1996. The ITMRA and FARA were subsequently designated the Clinger Cohen Act of 1996 (CCA), encompassing both. This is the first time in law that Chief Information Officers are established in government agencies, along with listing their roles and responsibilities. (Clinger Cohen Act of 1996, Title 40 – editors note)

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. (JP-1)

Command, Control, Communications, and Computers (C4) - The Marine Corps Headquarters Department responsible for planning, directing, coordinating, and overseeing C4 and IT capabilities that support the warfighting functions. The Department influences the combat development process by establishing policy and standards for developing the enterprise architecture. (C4 Website)

Communities of Interest (COIs) - A collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. (9 May 2003 DCIO DOD Net-Centric Data Strategy)

Continuity Of Operations (COOP) - The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. (JP 1-02)

Confidentiality - Assurance that information is not disclosed to unauthorized individuals, processes, or devices. (CNSSI No. 4009)

Cyberspace - A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and imbedded processors and controllers. (SECDEF Memo: Definition of Cyberspace, 12 May 2008)

Cyberspace Operations - The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (GIG). (JP 1-02)

Defense Acquisition System (DAS) - The management process by which the Department of Defense provides effective, affordable, and timely systems to the users. (DOD 5000.01)

Defense-in Depth - The DOD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness. (DODD 8500.01E)

Defense Information Technology Infrastructure Library (DITIL) - The DOD approach to implementing ITIL starting with the development of a Service Catalog, then addressing IT processes. DITIL will leverage current efforts such as the Defense Information Enterprise and GIG. (DITIL Portal). *(Enterprise IT Services Management is a related term)*

Department of Defense Information Enterprise (DOD IE) - The DOD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DODD 8000.01)

Disaster Recovery (DR) - The ability to recover from the loss of a complete site, whether due to natural disaster or malicious intent. Disaster recovery strategies include replication and backup/restore. Disaster Recovery is a subset of the overall IT Service Continuity Management Process which supports the overall business continuity management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support, and service desk) can be recovered within required, and agreed, SLAs. (MCEITS CPD, 17 FEB 2010, Ver. 1.4)

Distributed Services - A term used to describe the provision of enterprise level IT services to a wide number of subscribers, users, and other systems that are non-centralized, geographically dispersed and access services using wide varieties of bandwidth. (NIST)

Enterprise Architecture - A strategic information asset base that defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. EA includes a baseline architecture, a target architecture, and a sequencing (transition) plan. (DODI 8410.02)

Enterprise Land-Mobile Radio (ELMR) - This is a funded Marine Corps Program of Record to replace existing non-compliant SE LMR, repeaters sites, and C2 devices at each garrison installation with modern, digital, trunked radio systems at all bases, posts, and stations across the Marine Corps. ELMR supports positive command and control, safety of life/safety of flight for training units and exercise control groups, Installation Commander's safety of life and preservation of property missions and Law Enforcement, Fire and Emergency Services, Force Protection, and Range Control Radio interoperability capability between Installation Commander's First Responders w/ Local, State, and Federal responders. (ELMR POM 12 Baseline Brief)

Expeditionary Force Development System (EFDS) - A process, led by the Deputy Commandant for Combat Development and Integration, which guides the identification, development, and integration of warfighting and associated support and infrastructure capabilities for the MAGTF. (MCO 3900.15B)

Federated Enterprise Architecture - An approach for enterprise architecture development that is composed of a set of coherent but distinct entity architectures—the architectures of separate members of the federation. The members of the federation participate to produce interoperable, effectively integrated enterprise architecture. The federation sets the overarching rules of the federated architecture, defining the policies, practices, and legislation to be followed, as well as the inter-federate procedures and processes, data interchanges, and interface standards, to be observed by all members. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission. (DOD Information Enterprise Architecture 1.1)

Global Information Grid (GIG) - The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. (JP 6-0)

High Availability (HA) - Availability is the ratio of time that a service is available to total time. Availability can be expressed as mean time between failure (MTBF) and mean time to repair. Availability is typically expressed in percentage of time the system is available or in downtime per year. The two methods of expressing availability are "number of nine's" or availability percent. HA for DoD is usually expressed as "5 nines or 99.997%. (DOD Unified Capabilities Requirements, 2010, Sect. 5.3.1.7.6).

Information Assurance (IA) - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-13)

Information Assurance Workforce - The DOD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions listed in DOD 8570.01-M. These individuals are considered to have significant "security responsibilities" and must receive specialized training and be reported per the Federal Information Security Management Act and this Manual. (DOD 8570.01-M)

Information Environment - Aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information itself. (CNSSI No. 4009)

Information Technology Steering Group (ITSG) - Conducts value and risk assessments of IT investments to inform the Program Objective Memorandum (POM) development process and portfolio management approach. The ITSG coordinates the application and use of IT consistent with overall objectives. (ITSG Charter)

Initial Capabilities Document (ICD) - Summarizes a Capabilities Based Assessment (CBA) and justifies the requirement for a materiel or non-materiel approach, or an approach that is a combination of materiel and non-materiel, to satisfy specific capability gap(s). It identifies required capabilities and defines the capability gap(s) in terms of the functional area, the relevant range of military operations, desired effects, time, and doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) and policy implications and constraints. The ICD summarizes the results of the DOTMLPF and policy analysis and the DOTMLPF approaches (materiel and non-materiel) that may deliver the required capability. The outcome of an ICD could be one or more joint DOTMLPF Change Recommendations (DCR) or recommendations to pursue materiel solutions. (CJCSI 3170.01G)

Integrity - Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (CNSSI No. 4009)

Internet Protocol (IP) - Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (CNSSI No. 4009)

Interoperability - The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information technology and National Security System interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with information assurance. (DODD 4630.05)

International Standards Organization (ISO) - The ISO comprises national standards bodies representing 148 countries and serves a variety of functions. It facilitates communication and cooperation among its members, eases the distribution of scientific and technical information on standards and standardization, operates over 2,850 technical groups devoted to standards and other commercial and industrial research, and maintains online databases covering international standards and other organizational activities. (ISO Website)

IT Regionalization – The Marine Corps practice of developing Regional Network Operation Centers (RNOSCs) and the MAGTF IT Service Centers (MITSCs) in CONUS and OCONUS in order to better and more quickly deploy network oversight and control. (Integration Communications Strategy)

IT Service – A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's business processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement. (ITIL Service Strategy)

Joint Capabilities Integration and Development System (JCIDS) - A Chairman of the Joint Chiefs of Staff process to identify, assess, and prioritize joint military capability needs. The JCIDS process is a collaborative effort that uses joint concepts and integrated architectures to identify prioritized capability gaps and integrated DOTMLPF solutions (materiel and non-materiel) to resolve those gaps. (DODD 4630.05)

Marine Air-Ground Task Force (MAGTF) - The Marine Corps principal organization for all missions across the range of military operations composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the Marine air-ground task force (MAGTF) are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a combat service support element. The four core elements are categories of forces, not formal commands. The basic structure of the MAGTF never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs to be assigned. (JP 1-02)

Marine Corps Enterprise Information Technology Services (MCEITS) - The "Enterprise Services" component of the Marine Air Group Task Force (MAGTF) Command and Control (C2) construct and System of Systems that enables the end-to-end C2 capability for the Marine Corps. MCEITS closes the gap between emerging DOD Net-Centric infrastructure and the current Marine Corps legacy IT architecture and infrastructure. (Integrated Communications Strategy v2.5)

Marine Corps Enterprise Network (MCEN) - the Marine Corps' network-of-networks and approved interconnected network segments. It comprises policy, governance, people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations.

Marine Corps Information Technology Environment (MCITE) - the environment that consists of the MCEN and all other information technologies owned, operated, controlled, and/or governed by the Marine Corps. It includes USMC IT assets that are inherent and not inherent to the MCEN, and those USMC IT assets that are part of other networks or stand-alone systems.

Marine Corps Information Environment (MCIE) - the broad domain for all forms of communication. It comprises Marine Corps data, information, knowledge, and the management processes for ensuring their effective distribution and use across the Marine Corps and with mission partners. The MCIE often leverages, but does not always depend upon technology and communications systems to facilitate the flow of data, information, and knowledge across the enterprise.

Marine Corps Intelligence Surveillance and Reconnaissance Enterprise (MCISR-E) - The multi-level intelligence component of the MCIENT. MCISR-E provides improved end-user access to non-organic intelligence resources, and expands data sharing with other functional areas and with Joint, Allied, and Coalition mission partners.

Marine Corps Vision and Strategy (MCV&S) 2025 - Serves as the principal strategic planning document for the Marine Corps and reflects the legislated roles, functions, and composition. Derived from strategic guidance at the national and departmental levels, it illustrates the Corps' utility and value within the joint warfighting community. It informs all Marines where we intend to take our Corps, to give combatant commanders a concept of how we might best be employed, and to provide our civilian leadership a reference point as to how we see Marine Corps contributions to national defense in the coming years and decades. (MCV&S 2025)

Marine Requirements Oversight Council (MROC) - The MROC advises the Commandant of the Marine Corps on policy matters related to concepts, force structure, and requirements validation. It is chaired by the Assistant Commandant of the Marine Corps (ACMC) and is composed of permanent and associate members. The permanent members are: ACMC, Deputy Commandants for Programs and Resources (P&R), Manpower and Reserve Affairs (M&RA), Aviation (A), Plans Policies and Operations (PP&O), Installation and Logistics (I&L), and Combat Development and Integration (CD&I).

Mission Partners - Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. (DODD 8000.01)

Net-centric Enterprise Services (NCES) - An acquisition program that identifies, develops, and implements GIG CES. GIG CES include application, discovery, user assistant, collaboration, storage, mediation, messaging, enterprise service management, and information assurance/security. NCES enables the secure, agile, robust, dependable, interoperable data-sharing environment for DOD where warfighter, business, and intelligence users share knowledge on a global network. This, in turn, facilitates information superiority, accelerates decision-making, effective operations and net-centric transformation. (www.disa.mil)

Network – Information system implemented with a collection of interconnected nodes. (CNSSI) No. 4009)

Network Operations (NetOps) - The DOD-wide operational, organizational, and technical capabilities for operating and defending the GIG. NetOps includes, but is not limited to, enterprise management, net assurance, and content management. NetOps provides commanders with GIG situational awareness to make informed command and control decisions. GIG situational awareness is gained through the operational and technical integration of enterprise management and defense actions and activities across all levels of command (strategic, operational, and tactical). (DODI 8410.02)

Networking on the Move (NOTM) concept - A family of systems that promotes/supports an OTM terrestrial, celestial, and aerial network providing Beyond Line of Sight (BLOS) extensions using a combination of existing, planned, and new initiatives.

Non-repudiation - Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. (CNSSI No. 4009)

On-the-Move - Movement phase; in an operation using military forces, the period when various elements of forces move from points of embarkation to the operational area; or when military forces move from place to place while retaining the ability to fulfill their primary mission. (DOD Dictionary, 2009).

Operational Control (OPCON) - 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 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. (JP-1)

Planning, Programming, Budgeting, and Execution Process (PPBE) - The formal process for formulation of the DOD budget request. Besides preparing a budget for Congress, the PPBE process is also a mechanism for creating a long-range financial plan that relates Defense spending to assessments of potential military threats, as summarized in the President's National Security Strategy and the Quadrennial Defense Review. (UOSD(C) Website)

Portfolio Management - The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability. (DODD 8114.01)

Reachback - An effective reach-back communication system enables the Commander to conduct dispersed operations in a nonlinear battle space. The communications system must be interoperable, agile, trusted, and shared, taking advantage of "reach-back" to exploit non-organic capabilities inherent in other organizations. (Definition provided for USMC Vision & Strategy 2025 Implementation Planning Guidance Task 13.G)

Risk - Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability. (CNSSI No. 4009)

Self-Forming/Self Healing - Core elements of service-discovery research (at NIST) these two properties are key to characterizing the behavioral and performance properties of service-discovery protocols when deployed in demanding situations. The ability for networks be they mobile or ad-hoc to improve performance of service-discovery protocols in volatile and hostile environments. (NIST, 2009)

Standardization Agreement (STANAG) - Establishes processes, procedures, terms, and conditions for common military or technical procedures or equipment between the member countries of the alliance. Each NATO state ratifies a STANAG and implements it within their military. STANAGs also form the basis for technical interoperability between a wide variety of communication and information (CIS) systems essential for NATO and Allied operations. (NATO)

STANAG 4609 - Full motion video NATO standard. (NATO)

Tactical Control (TACON) - 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. (JP-1)

Threat - Any circumstance or event with the potential to adversely impact an [Information System] through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (CNSSI No. 4009)

Transport Layer - The network transport layer provides "end-to-end" connections, reliability, and flow control of data transfer services. This control is managed by ports and protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), Stream Control Transfer Protocol (SCTP) and Secure Socket Layer (SSL) and Transport Layer Security (TLS). This layer of the DOD communications model manages the transportation of data, establishes the connection between hosts to exchange already formatted data and controls the reliability of a given link through flow control. (OSI Reference Model)

Universal Needs Statement (UNS) - Identifies operational enhancements, opportunities, and deficiencies in terms of a stated capability set. Opportunities may include new capabilities, improvements to existing capabilities, and elimination of redundant or unneeded capabilities. (MCO 3900.15B)

Urgent Universal Needs Statement (UUNS) - An exceptional request from a combatant command-level Marine component commander for an additional warfighting capability critically needed by operating forces conducting combat or contingency operations. Failure to deliver the capability requested by the U-UNS is likely to result in the inability of units to accomplish their missions or risks increased probability of casualties and loss of life. (MCO 3900.15B)

6.2 REFERENCES

Capability Development Document for Marine Corps Enterprise Information Technology Services (MCEITS). 2007

Capstone Concept for Joint Operations. 2009

Initial Capabilities Document for Global Information Grid 2.0. 2009

ITIL Service Strategy. 2007

Joint Publication 1-02, DOD Dictionary of Military Associated Terms. 2009

Marine Corps Functional Concept for Command and Control. 2009

Marine Corps Vision & Strategy 2025. 2008

Nissen, M. (2006). *Harnessing knowledge dynamics: Principled organizational knowing & learning*. Hershey: IRM Press.

USMC Service Campaign Plan. 2009

USMC Cyberspace Concept. 2009

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS
Headquarters, U.S. Marine Corps, Washington, DC
C4