NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE FRAMEWORK FOR AN INFORMATION TECHNOLOGY STRATEGIC ROADMAP FOR THE UNITED STATES MARINE CORPS: HOW CURRENT ACQUISITIONS ALIGN TO THE CURRENT STRATEGIC DIRECTION OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF THE NAVY, AND UNITED STATES MARINE CORPS

by

Richard Garcia
Joshua Sloan

June 2008

Thesis Advisor: Glenn Cook
Associate Reader: Cary Simon

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE The Framework for an Information Technology Strategic Roadmap for the United States Marine Corps: How Current Acquisitions Align to the Current Strategic Direction of the Department Of Defense, Department of the Navy, and United States Marine Corps

5. FUNDING NUMBERS

6. AUTHOR(S) Richard D. Garcia & Joshua K. Sloan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the DoD or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Development and implementation of a 21st century Marine Corps information technology (IT) roadmap may comprise a "tipping point" for future warfighting effectiveness. This thesis begins the basis for a framework for an information technology strategic roadmap for the United States Marine Corps.

This thesis depicts how current acquisition programs align to current IT strategies. A premise, based on the theoretical foundation of general systems theory is that the alignment of multiple IT strategic plans, roadmaps and strategies positively affects system effectiveness. IT strategies are identified and compiled from Department of Defense (DoD), Department of the Navy (DoN), and United States Marine Corps (USMC) overarching strategic documents. Major acquisition programs for the DoD, DoN, and USMC are selected and summarized. These selected current acquisition programs are related to the identified IT strategies from the DoD, DoN, and USMC overarching strategic documents in terms of their interrelationships or alignment. Based on the research, this thesis provides recommendations to current acquisition programs to better align with the current direction of the DoD, DoN, and USMC IT strategy, and future research opportunities.

14. SUBJECT TERMS Alignment, IT Strategies, Roadmap, National Defense Strategy, DoD CIO Strategic Plan, Enterprise Transition Plan, Sea Power 21, DoN Information Management/Information Technology Strategic Plan, Marine Corps Strategy 21, Commandant's Planning Guidance, USMC Concepts and Programs, Transformation, Net-Centric, Information Operations, IA, Information Sharing, Horizontal Integration, Governance, DIMHRS, JC2, Navy ERP, GCCS-M, MCEITS, GCSS-MC

15. NUMBER OF PAGES 157

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

THE FRAMEWORK FOR AN INFORMATION TECHNOLOGY STRATEGIC ROADMAP FOR THE UNITED STATES MARINE CORPS: HOW CURRENT ACQUISITIONS ALIGN TO THE CURRENT STRATEGIC DIRECTION OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF THE NAVY, AND UNITED STATES MARINE CORPS

Richard D. Garcia
Major, United States Marine Corps
B.A., Park University, 1996

Joshua K. Sloan
Captain, United States Marine Corps
B.S., Iowa State University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Authors: Richard D. Garcia

Joshua K. Sloan

Approved by: Glenn Cook
Thesis Advisor

Cary Simon
Associate Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Development and implementation of a 21st century Marine Corps information technology (IT) roadmap may comprise a “tipping point” for future warfighting effectiveness. This thesis begins the basis for a framework for an information technology strategic roadmap for the United States Marine Corps.

This thesis depicts how current acquisition programs align to current IT strategies. A premise, based on the theoretical foundation of general systems theory is that the alignment of multiple IT strategic plans, roadmaps and strategies positively affects system effectiveness. IT strategies are identified and compiled from Department of Defense (DoD), Department of the Navy (DoN), and United States Marine Corps (USMC) overarching strategic documents. Major acquisition programs for the DoD, DoN, and USMC are selected and summarized. These selected current acquisition programs are related to the identified IT strategies from the DoD, DoN, and USMC overarching strategic documents in terms of their interrelationships or alignment. Based on the research, this thesis provides recommendations to current acquisition programs to better align with the current direction of the DoD, DoN, and USMC IT strategy, and future research opportunities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank Mr. Clint Swett (Director, Technology Services Organization, DFAS-KC) and Major Jeffrey Thiry (Deputy Director, Technology Services Organization, DFAS-KC) for their help and support. Their guidance proved invaluable in shaping our thoughts and perceptions of the role of Information Technology within the Marine Corps. Special thanks to Mr. Glenn Cook and Dr. Cary Simon for giving us the latitude and support to write this paper.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MARINE CORPS INFORMATION TECHNOLOGY STRATEGIC DIRECTION

Development and implementation of a 21st century Marine Corps information technology (IT) roadmap may comprise a "tipping point" for future warfighting effectiveness (Gartner, 2006). Effectiveness is defined as "productive of results", including adaptation to a changing external environment (Merriam-Webster, 2007). U.S. government and defense IT requirement purchases typically require longer lead-times than the private sector due partly to the five to seven year Planning, Programming and Budgeting cycle and recurring political cycles (Gartner, 2006).

This thesis describes Department of Defense (DoD), Department of the Navy (DoN), and United States Marine Corps (USMC) IT themes from overarching strategic documents. The point is to examine interrelationships or alignment with selected acquisition programs. A premise, based on the theoretical foundation of general systems theory is that the fit or alignment among multiple IT strategic plans, roadmaps and strategies positively affects overall performance or system effectiveness. The reverse would theorize that the extent to which multiple competing DoD, DoN, and USMC IT strategies do not interrelate, or are incongruent will degrade overall effectiveness. An alignment summarization is provided in later chapters, which also depicts apparent gaps between strategy documents and selected acquisition programs.

According to Gartner (2006) - a leader in IT research and advisory - government IT strategy plans often fall at two ends of a "specificity spectrum." At one end are plans containing broad goals emphasizing the criticality of IT to the success of an organization. There may or may not be specific linkages to changing political agendas. Often, details about what exactly will be done, how and when it will occur, and expected performance improvements or results are typically insufficient or missing. (Gartner, 2006)

At the other end of the spectrum are IT strategic plans tailored for system engineers, network administrators, information architects and application developers. These types of plans often result in a laundry list of proposed technology spending plans. Although these types of IT strategic plans may well depict cost and spending parameters, they may simultaneously provide little useful insight for non-technological stakeholders and managers. Gartner (2006) identifies these specifically as business owners and process managers, budget and oversight analysts and managers. Typically lacking are descriptions clarifying how IT investments are specifically linked to business or program improvement goals and priorities. While spending and technologically intense IT strategic plans designed for system engineers, network administrators, information architects and application developers can be useful, they may not satisfy the needs and expectations of stakeholders outside the IT field. (Gartner, 2006)

An expressed driver for the Marine Corps to create an IT road map is to achieve strong alignment between business and information technology strategies. This attempt to align business and IT strategies has been recognized as a crucial

issue which increases in importance over time (Gartlan and Shanks, 2007). Alongside the intended alignment of business and IT strategies, the Marine Corps intends to develop an integrated, Enterprise Resource Plan (ERP). An ERP is meant to integrate all relevant data and processes across and within applicable agencies into a unified system (Center for Digital Government, 2005). Figure 1 depicts such a system.

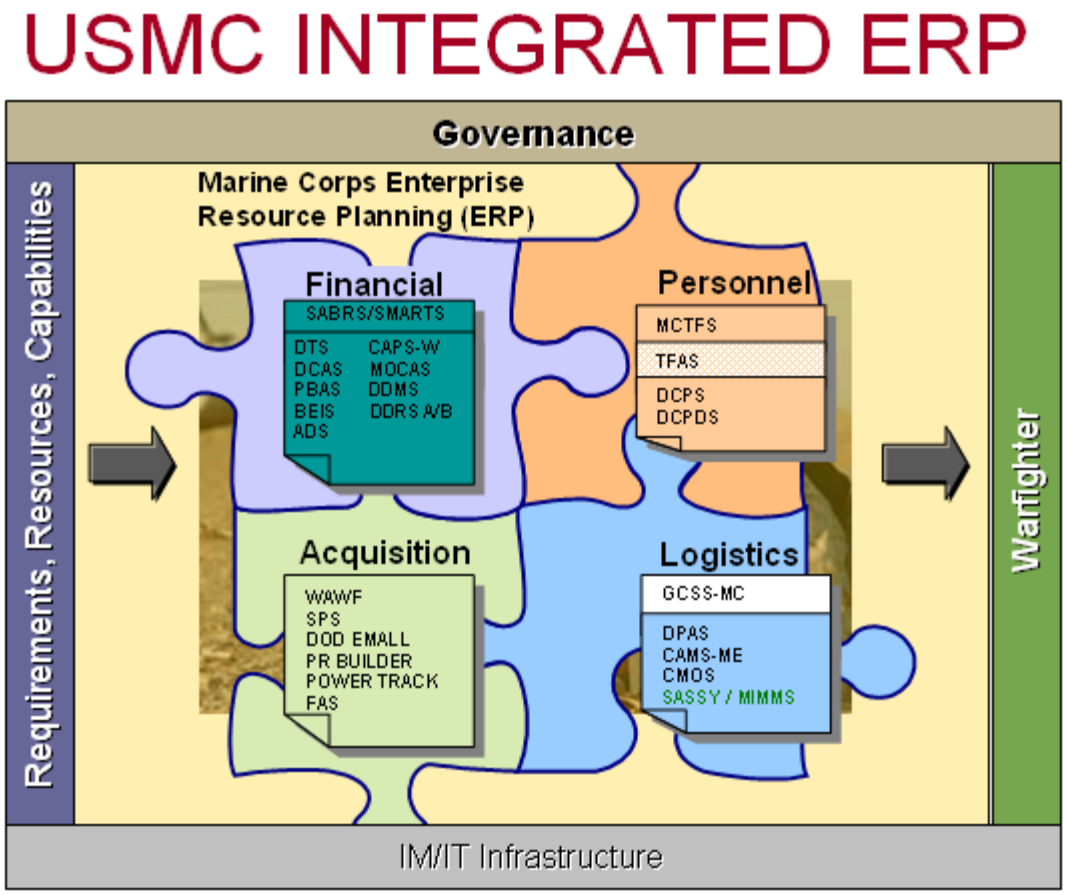

Figure 1. USMC ERP (TSO, 2007)

B. RESEARCH QUESTIONS

The following research questions were formulated and analyzed to assist ongoing efforts to develop and implement an IT strategic roadmap which meets the needs and expectations of relevant stakeholders. Done poorly, an IT strategic plan runs the real risk of ending up as "shelfware," useful primarily for satisfying legal mandates and passing funding compliance hurdles. (Gartner, 2006)

Research Questions

1. What is the current and future plan or roadmap for Marine Corps IT strategy, including the extent to which current and future strategic themes align with applicable DoD, DoN and USMC acquisitions?

2. What are the identifiable IT strategic themes expressed in DoD, DoN and USMC IT strategic documents?

3. To what extent are aspects of DoD, DoN and USMC IT strategies aligned with selected acquisition programs?

4. To what extent are their gaps or incongruencies among DoD, DoN and USMC IT strategies and acquisition programs?

5. How can the USMC IT strategic roadmap be designed and communicated for optimal impact and effectiveness?

C. POTENTIAL BENEFITS

A well-designed and communicated IT strategic road map can be a crucial enabler for improving and transforming defense business systems and acquisitions. Efficient and effective defense business systems directly impact human resource management, financial, and technological development and procurement systems, all of which contribute to defense readiness.

Granted that the USMC core competency is warfighting and not IT. Improving and fielding cutting-edge information technology systems however, has become a 21st century axiom of success. Indeed, Al Quaida mounts an apparently successful internet recruiting campaign complete with blogs and chatrooms. Therefore, designing and implementing a powerful IT infrastructure is crucial for the Marine Corps to excel in conventional, irregular and hybrid future wars. An IT road map can provide the planning documents needed to sustain information superiority, thereby enabling warfighters to focus on fighting wars.

To the extent that the DoD is the largest employer on the planet, improving, integrating and communicating overarching IT strategies is essential for making an array of complex business decisions.

Benefit: *Strategic acquisitions of IT requirements.*

An IT strategic road map will enable a cost effective improvement for IT business systems portfolio management. There are many variables which impact the management of the IT portfolio such as cost, implementation, manageability,

flexibility, performance, and capabilities. These variables must be addressed strategically for any project to be a success.

Benefit: *Allow stakeholders to identify gaps between programs and strategies.*

The USMC's core competency is warfighting, not IT. Although, it is understood that in order to provide the warfighter with the best resources available the USMC must continue to improve its IT infrastructure. An IT road map will enable the USMC to ensure that the IT portfolio is handled efficiently and timely allowing the warfighter to focus on fighting wars.

Benefit: *More effective governance of IT portfolios.*

By identifying and understanding the overarching IT strategies the DoD, DoN, and USMC can make precise business decisions regarding IT systems to meet current and future organization requirements, thus minimizing unneeded IT system upgrades, development, and major acquisitions.

Benefit: *A framework for a successful IT strategic road map.*

Understandably, every organization must have a plan for success. By developing a methodology for an IT strategic road map, the Marine Corps will be able to successfully plan its current and future IT acquisitions as well as set a plan for implementation of new acquisitions.

D. METHODOLOGY

The research for this thesis was conducted in a methodology that is relatively straightforward. The qualitative research methodology of this thesis entailed the collection, identification, examination, and synthesis of relevant DoD, DoN, USMC documents, pertaining to requirements and standards contained in the strategic documents. From these strategic documents, IT themes were identified and discussed. Thus, allowing for the compilation of relevant IT themes identified. Additionally, there was an examination of six current IT related acquisition programs being developed and/or sponsored by DoD, DoN, and USMC strategic and operational planners. The examination of current acquisition programs illuminates the alignment and gaps between those current acquisitions programs and compiled IT themes.

Further supplementation of the gathered information was obtained to provide the details of other examples, relevant and current IT strengths, and needed future areas of improvement. Conclusions were drawn concerning relative areas of alignment and recommendations offered to assist managers and practitioners in ongoing IT infrastructure developments. Finally, this methodology allowed for future work in the design of an USMC IT roadmap.

E. ORGANIZATION OF STUDY

Chapter I describes the motivation for the study related to the Naval Postgraduate School masters degree in Information Technology (IT), and the concept of emerging strategic road maps for defense, Navy and Marine Corps

institutions. Also described are research questions, benefits of the study, and methodology for data collection and analysis. Chapter II reviews selected defense, Navy and Marine Corps strategic documents in terms of IT direction and related strategies. Chapter III summarizes six, IT related acquisition programs being developed and/or sponsored by defense, Navy and Marine Corps organizations. Specifically, one business system and one tactical system are addressed for each enterprise. Chapter IV analyses relative alignment between IT strategic themes and acquisition programs, and Chapter V includes gap descriptions, recommendations to improve alignment and future research areas.

II. LITERATURE REVIEW

A. INTRODUCTION

This chapter describes strategy documents from the Department of Defense (DoD), Department of the Navy (DoN), and the United States Marine Corps. The documents are examined in terms of their implications for defense information technology (IT), particularly in terms of the vision, direction and interrelatedness of current and future defense IT strategies.

B. DEPARTMENT OF DEFENSE (DOD)

The following DoD documents provide general guidance on the overall IT framework, including various role clarifications and common processes governing, managing and planning IT roles and requirements (ETP, 2007): U.S. National Defense Strategy; DoD Chief Information Officer Strategic Plan; and the Enterprise Transition Plan. These documents are not step-by-step procedures for developing IT architecture or transitioning plan products or program acquisition documents. *Enterprise* is defined by Merriam-Webster (2007) as a unit of economic organization or activity; especially: a business organization. For purposes of this research, “enterprise” refers to a family of defense organizations; including their respective IT business strategies.

1. U.S. National Defense Strategy

National Defense Strategy produced by the Secretary of Defense is a repetitive, layered approach for describing and documenting overarching defense planning (unclassified) for the U.S. and its defense interests. The tone of the document reinforces conditions instrumental in defending national and international sovereignty, founded on the values of freedom, democracy, and economic opportunity. The strategy promotes close cooperation with selected global entities likewise committed to these broad goals. Both mature and emerging threats are addressed (National Defense Strategy, 2005). National Defense Strategy is partitioned in three sections detailing various strategic objectives, ways of accomplishing the objectives and implementation guidelines.

a. Information Technology Themes

A theme is defined by Merriam-Webster (2007) as a specific and distinctive quality, characteristic, or concern. National Defense Strategy contains four information technology themes described below.

- **Continuous Transformation Theme**

The term “transformation” implies radical change such that organizational strategies, structures, processes, culture and outcomes may take on markedly different properties, while preserving core defense values. Ackerman (1986) says that incremental or developmental change is fundamentally different from transformational change, but that organizations can transform through incremental

improvements, as well as strategies to transition from an old-state to a known, new-state. External environmental forces, trends and pressures can also intervene during and throughout any change process (Cook & Dyer, 2003).

National Defense Strategy describes the purpose of transformation as extending key advantages and reducing vulnerabilities and that, “continuous defense transformation is part of a wider governmental effort to transform America’s national security institutions to meet 21st-century challenges and opportunities.” According to National Defense Strategy, transformational change is not limited to operational forces. The DoD wants to change long-standing business processes within the Department to take advantage of information technology, i.e., a revolution in business affairs. Furthermore, the Department of Defense indicates its intention to transform international partnerships, including increasing collective capabilities, e.g., a 1,000 ship Navy (Federal Executive, 2007; National Defense Strategy, 2005)

- **Strengthen Intelligence Theme**

“Intelligence directly supports strategy, planning, and decision-making; it facilitates improvements in operational capabilities; and it informs programming and risk management” (National Defense Strategy, 2005). The National Defense Strategy looks at horizontal integration as a key priority in strengthening intelligence. The American Marketing Association (2007) defines horizontal integration as the expansion of a business by acquiring or developing businesses engaged in the same stage of marketing or distribution, e.g. the standard oil company's acquisition of

40 refineries, or an automobile manufacturer's acquisition of a sport utility vehicle manufacturer, or a media company's ownership of radio, television, newspapers, books, and magazines.

DoD strategy seeks to better fuse operations and intelligence, including diminishing institutional, technological, and cultural barriers, i.e., enabling personnel to better acquire, assess, and deliver critical intelligence to senior decision-makers and warfighters. In addition, it describes the importance of improving counterintelligence as crucial for ensuring long-term information dominance (National Defense Strategy, 2005).

- **Information Operations Theme**

Information Operations, as defined by Joint Pub 3-13, are actions taken to affect adversary information and information systems, while defending one’s own information and information systems. National Defense Strategy (2005) states that, “Cyberspace is a new theater of operations. Consequently, Information Operations (IO) is becoming a core military competency.” In short, successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates additional vulnerabilities; however, an adversary’s use of information networks and technologies creates opportunities to conduct offensive IO as well. “Developing IO as a core military competency requires fundamental shifts in processes, policies, and culture” (National Defense Strategy, 2005).

- **Network Centric Operations Theme**

Network Centric Operations, also known as Network Centric Warfare, is a key component of DoD planning for strategic, operational, and tactical military transformation (Wilson, 2007). Former Chief of Naval Operations, Admiral Jay Johnson, called Network Centric Operations "a fundamental shift from platform-centric warfare." Alberts, Garstka, and Stein (2000) define Network Centric Warfare as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, Network Centric Warfare translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

"The foundation of our operations proceeds from a simple proposition: the whole of an integrated and networked force is far more capable than the sum of its parts" (National Defense Strategy, 2005). National Defense Strategy describes how ongoing advances in information technology and communication holds promise for networking highly distributed joint and combined forces. The strategy indicates that network-centric operational capability is achieved by linking compatible information systems with usable data. "Beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes by giving all users access to the latest, most relevant, most accurate information" (National Defense

Strategy, 2005). A network-centric force transformation may require fundamental changes in processes, policy, and culture to provide the necessary speed, accuracy, and quality of decision-making critical to future success (National Defense Strategy, 2005).

2. Chief Information Officer DoD Strategic Plan

The Chief Information Officer (CIO) Strategic Plan developed by the DoD CIO attempts to provide the direction and design needed to accomplish the Net-Centric vision, including developing the enabling capabilities required in National Defense Strategy. The plan identifies actions deemed critical for transforming DoD operations from platform/organization-centric to Net-Centric. It provides a common understanding of the near and mid-term actions required to meet the vision and extend Net-Centricity across the Defense Information Enterprise. The plan focuses on nine areas which the DoD CIO deems necessary to complete a transformation to Net-Centric operations. Each focus area includes a description of issues or needs that led to its formulation, actions required from various organizations, and applicable components of the doctrine, organization, training, material, leadership/education, personnel, and facilities (DOTMLPF) listed for each action. (CIO Strategic Plan, 2006)

a. Information Technology Themes

- **Net-Centric Culture Theme**

A Net-Centric culture revolves around the belief that the information one element produces may be useful to

another element for any reason, seen or unforeseen. Thus, the information solution that enables better decision-making is based on the assumption that information made available to the enterprise will increase combat power in unspecified forces. (Krieg, 2007)

The CIO (2007) in the DoD Net-Centric Services strategy describes the Department's commitment to achieving Net-Centric operations. It further explains the foundation of Net-Centric culture as being the ability for users to obtain the required and available information and applications when and where they are needed.

The CIO Strategic Plan discusses accelerating the Net-Centric culture by developing operational concepts that exploit the power of emerging information sharing capabilities and validate these concepts through experiments and demonstrations. A fundamental objective in the DoD's Net-Centric strategy, as stated in the CIO Strategic Plan, is to move "power to the edge." The edge refers to the individual operator or user who might be an intelligence analyst at a Combatant Command, a human resources specialist at a military base, or a warfighter on the streets of Baghdad. This objective is based on the supposition that the deployed warfighter has the greatest need for timely, relevant, and accurate information and, in many cases, is the best provider of information to support mission accomplishment (CIO Strategic Plan, 2006).

The CIO Strategic Plan continues to describe that Net-Centric culture not only applies to the operational community, but also to the budgeting and acquisition communities. Net-Centric culture is about the coordination of the current disjointed approaches to identifying,

acquiring, engineering, developing, testing, evaluating, integrating and fielding joint and coalition Command, Control, Communications and Computer (C4) capabilities (CIO Strategic Plan, 2006).

- **Information Assurance (IA) Theme**

Information Assurance as defined by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) is: Information Operations (IO) that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation (obtainable, complete, genuine, discrete, and trustworthy from Merriam-Webster (2007)). This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities (Maconachy, Ragsdale, Schou & Welch, 2001).

DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense (2004), and the DoD Net-Centric Data Strategy (2003) goals include making data visible, accessible, understandable, trusted, and interoperable. Accordingly, the CIO strategy describes information that is visible, accessible, understandable and trusted as a force multiplier. The DoD Dictionary of Military Terms (2008) defines a force multiplier as a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment.

Furthermore, the goal of the CIO strategy when dealing with information assurance is to realize the efficiencies gained by understanding the meaning of data and using it in

a way that maximizes the effectiveness of military operations without overloading the warfighter with unusable information. Additionally, the CIO describes securing the information as mission assurance by protecting information, defending and keeping networks operational, acquiring trusted software, providing integrated situational awareness, transitioning and enabling IA capabilities, and creating IA awareness within the workforce (CIO Strategic Plan, 2006).

- **Networking the Warfighter Theme**

The DoD CIO (2006) sees networking the warfighter as providing an operating environment based on the DoD's major networking and C2 programs and coordinated Net-Centric operations procedures. By continuing the major programs and initiatives, such as the Defense Information Systems Network (DISN) and the Global Information Grid (GIG) expansion, as well as evaluating acquisition programs based on their consistency with the Net-Centric strategy, the CIO (2006) perceives this as the key to supporting the warfighter with Net-Centric operations.

- **Strengthen Intelligence Theme**

The DoD National Defense Strategy emphasizes the importance of sharing intelligence information. Consequently, the DoD CIO's Strategy (2006) calls for adjusting policies, modifying practices, and implementing tools such as Distributed Common Ground/Surface System (DCGS) to make quality intelligence data, both raw and processed, more widely and rapidly available to the warfighter.

When dealing with multi-agency, multinational and joint environments there are substantial challenges relating to information security involving the sharing of information. Thus, the CIO's Strategic Plan (2006) calls for a new and innovative approach to security risk management by building a secure, seamless network that responds to the vision of the Net-Centric strategy leading to effective intelligence information sharing (CIO Strategic Plan, 2006).

- **Information Sharing Theme**

The DoD Information Sharing Strategy (2007) defines Information Sharing as, "Making information available to participants (people, processes, or systems)." Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.

The CIO Strategic Plan (2006) describes the need to implement methods to manage the transition from today's information-sharing model, which is focused on interconnecting physical networks separated by classification, to a more Net-Centric model, which allows information sharing on the basis of classification and role-based access. This includes how to make information available to non-DoD partners and how to develop enterprise services, both of which are often complicated by use of different IT standards and data formats, different rules for releasing information and protecting network assets, and even use of different languages to communicate among foreign partners.

- **Aligning IT investments with Warfighting Strategy Theme**

The Clinger-Cohen Act of 1996 calls for wise IT investments and as such, has been the cornerstone of IT investments throughout the DoD. The DoD has gone a step farther by establishing the Information Technology Portfolio Management Directive of 2005, which established the roles and responsibilities throughout DoD for managing IT as portfolios of investments. Furthermore, these portfolios represent related systems that cross Military Services and Agency boundaries to deliver capabilities to warfighters (CIO Strategic Plan, 2006).

The concept of portfolio management, as stated in the CIO Strategic Plan, is to maximize outcomes and minimize costs for DoD investments. Reducing cost by eliminating duplicate and legacy systems resulting in the recapitalization of those funds saved to better support military operations. Additionally, the CIO's Strategic Plan (2006) describes the success of IT portfolio management as clearly articulating the responsibilities for the development and implementation of IT services among the IT portfolios.

- **Seamless Defense Business Infrastructure Theme**

As stated in the DoD Business Transformation Agency's (BTA) 2006 Annual Report to Congressional Defense Committees; "Today, a seamless defense business infrastructure is critical to support responsive, agile military operations. The goal for Defense Business Transformation is to provide our U.S. Armed Forces, what they need—when they need it—where they need it." In support

of the BTA and in compliance with its standards and policies, the DoD CIO Strategic Plan (2006) supports the identification and monitoring of existing and future business systems as well as the development of the GIG infrastructure. This infrastructure will enable interoperation and interconnection of business systems and applications when they need to exchange information, expose functionality, or consume information across federation boundaries (CIO Strategic Plan, 2006).

3. Enterprise Transition Plan (ETP)

Because the Department of Defense (DoD) is perhaps the largest and most complex organization in the world and manages a budget more than twice that of the world's largest corporation, it is logical that it would look for ways to improve business processes and results. In short, DoD's expanding and changing missions translates into even greater capability requirements in terms of agility, adaptation, flexibility and accountability. To help guide this undertaking, the Business Transformation Agency (BTA) of the DoD, whose mission is to guide the transformation of business operations throughout the DoD and to deliver Enterprise-level capabilities that align to warfighter needs (BTA, 2007), released its first integrated Enterprise Transition Plan (ETP) September 30, 2005, including subsequent annual releases. The ETP describes a systematic approach for the transformation of business operations within the DoD (BTA, 2007). This ETP is the first time that the DoD has provided its internal and external stakeholders

a comprehensive view of the systems and initiatives intended to transform the largest business entity in the world (ETP, 2007).

The ETP is organized into five sections. Section one describes the overview and perspective of the Defense Business Transformation. Section two discusses the Core Business Missions which are about aligning business to support warfighters. Section three describes the Enterprise Transformation which is divided into Business Enterprise Priorities and Visibilities. Sections four and five explain individual component (Department of the Army (DoA), Department of the Navy (DON), Department of the Air Force (DoAF), Defense Logistics Agency (DLA), United States Transportation Command (USTRANSCOM), Defense Finance and Accounting Service (DFAS)) transformation overviews and the managing and tracking of information within these components (ETP, 2007).

a. Defense Business Transformation

Because business transformation requires a multi-faceted set of activities, especially in a large, complex, hierarchical organization, the ETP (2007) identifies five core elements necessary to achieve defense business transformation as strategy, culture, process, information, and technology. (ETP, 2007)

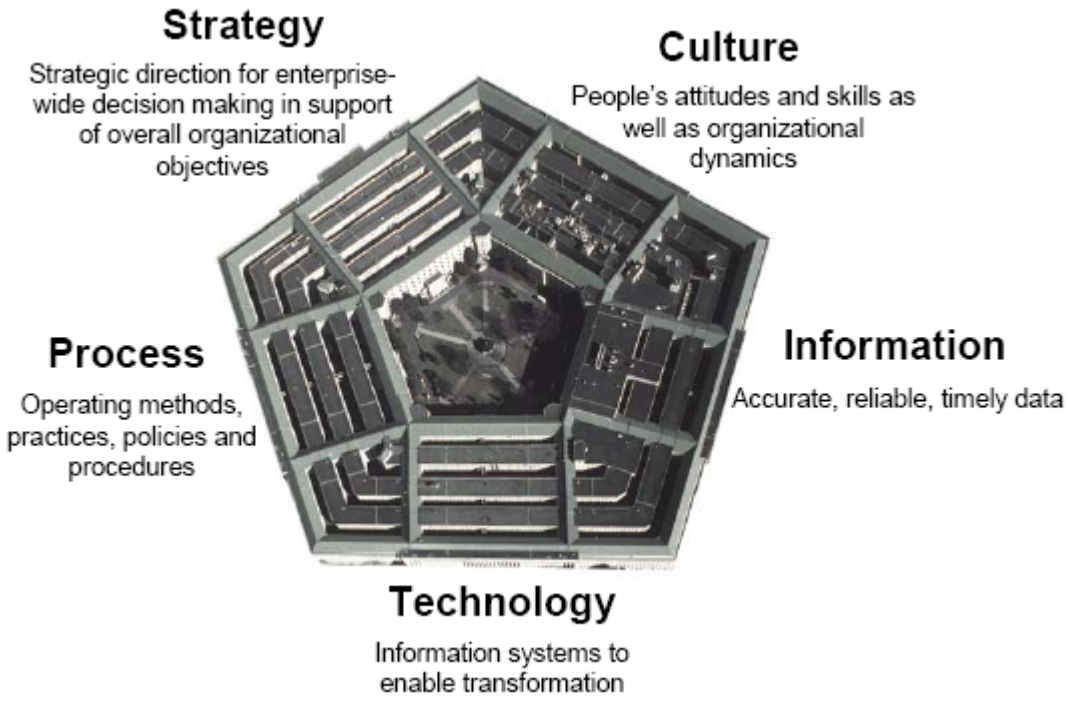

Figure 2. Core Business Transformation Elements (ETP, 2007)

(1) Strategy. The strategy area provides an understanding of the role, positioning, and focus for enterprise–wide decision making in support of organizational objectives. Defense business transformation is driven by four strategic objectives that shape priorities and serve as checkpoints to assess the usefulness of transformation efforts. The four strategic objectives are depicted below.

Figure 3. Business Transformation Strategic Objectives (ETP, 2007)

The role of strategic oversight for defense business transformation across the DoD is achieved through a process called tiered accountability. The ETP (2007) defines tiered accountability as a strategic concept that requires each tier in the DoD organizational hierarchy to focus on those requirements that are relevant for that specific tier, and leave the responsibility and accountability for other elements of business management and execution to other tiers in the organization. Tiered accountability focuses on the vertical aspects of the DoD organization, while ensuring the right people at the right level of the DoD organizational structure assume the appropriate level of responsibility for the relevant tasks associated with business transformation. According to the ETP (2007), the strategic use of the concept of tiered accountability has enabled both a more efficient and more effective means for the DoD to oversee its vast array of business system investments. Moreover, the

adoption of the concept of tiered accountability may represent a strategic shift in DoD's management culture (ETP, 2007).

(2) Culture. The ETP (2007) defines culture as people's attitudes and behaviors as well as the dynamics or organizational norms. There are of course subcultures within DoD. There is general acceptance that there have been culture shifts over the last several years in the area of business transformation. One of the major shifts was the development of the five Core Business Missions (CBMs) within the Business Mission Area. Business Mission Area can be generalized as an area of business that an organization has determined falls under one specific area of focus. DoD Directive 8115.01, Information Technology Portfolio Management, describes the BMA as ensuring that the right capabilities, resources, and materiel are reliably delivered to warfighters: what they need, where they need it, when they need it, anywhere in the world.

The development of the CBMs were in support of a DoD wide process of identifying joint needs, analyzing capability gaps, and implementing improvements that focus on supporting the warfighting mission. The CBMs are identified as: Human Resources Management, Weapon System Lifecycle Management, Materiel Supply and Service Management, Real Property and Installations Lifecycle Management, and Financial Management (ETP, 2007).

(3) Process. As discussed above, the DoD has espoused a cultural shift in the area of business transformation. More specifically, activities are shifting away from a focus on enhancing individual system capabilities toward activities designed to optimize end-to-end business processes (ETP, 2007).

Processes, as defined by Merriam-Webster (2007), are a series of actions or continuous operations conducive to an end. The ETP (2007) states processes are essential to business execution and as such, process improvements in themselves can augment transformation. The ETP (2007) describes process improvement as involving a continuous disciplined effort to decrease operational cost and cycle times, and reduce unnecessary work and rework, particularly by eliminating steps that add little or no value. The DoD's priority of process improvements are those that support the warfighter, e.g., those that provide capability improvements more rapidly, including returning equipment to use faster and cheaper (ETP, 2007).

(4) Information. While process transformation is focused on how business is conducted within the DoD, the ETP (2007) has determined that information transformation relates to the DoD's ability to leverage the results of those processes to make optimal decisions, as well as provide decision makers access to timely, reliable, and accurate information. The ETP (2007) continues to state that information transformation encompasses data definitions and business rules, but true

transformation may not be realized until those data standards become embedded in the processes and supporting systems.

(5) Technology. The DoD is investing significantly in IT business systems at both the enterprise and component organizational levels (ETP, 2007). The ETP (2007) describes information technology as providing a physical representation that enables and enforces the strategy, culture, process, and information elements of business transformation. The ETP (2007) continues by saying all of these elements are essential to achieving transformational results, and it is the IT portion of the overall solution that often ultimately delivers actual capabilities to the DoD community.

b. Core Business Missions

In an effort to identify joint needs, analyze capability gaps, and implementing improvements, the DoD developed five Core Business Missions (CBM) that focused strictly on supporting the warfighting mission. The five CBMs are Human Resources Management (HRM), Weapon System Lifecycle Management (WSLM), Material Supply and Service Management (MSSM), Real Property and Installations Lifecycle Management (RPILM), and Financial Management (FM). CBMs are meant to be integrated horizontally across all business functions (e.g., planning, budgeting, IT, procurement, maintenance) to provide end-to-end support and cross-coordination (ETP, 2007).

(1) Human Resources Management. The Human Resources Management (HRM) Core Business Mission area, as defined by the ETP (2007), is responsible for all Human Resource (HR) processes necessary to acquire, train, and prepare personnel to populate warfighter and support organizations. HRM goals are to improve and transform business practices and information systems to better support service members, civilian employees, military retirees, volunteers, contractors (in theater), other U.S. personnel, the warfighter and others with an agile, joint, Total-Force DoD Human Capital Strategy (ETP, 2007).

(2) Weapon System Lifecycle Management. The Weapon System Lifecycle Management (WSLM) Core Business Mission, as defined by the ETP (2007), encompasses the Defense Acquisition business processes that deliver weapon systems and automated information systems. The mission of the WSLM CBM is to execute Defense Acquisition, which is defined in the Defense Acquisition Guidebook (2004) as, activities that execute the conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions (ETP, 2007).

(3) Material Supply and Service Management. The Materiel Supply & Service Management (MSSM) CBM, as defined by the ETP (2007), manages supply chains for the provision of materiel supply and services to deploy, redeploy and sustain the warfighter, increase materiel

availability and maintain readiness of deployed and non-deployed forces. The goal of the MSSM CBM is to improve business practices and information systems to better support the warfighter with a more agile and effective supply chain (ETP 2007).

(4) Real Property and Installations Lifecycle Management. The Real Property and Installations Lifecycle Management (RPILM) Core Business Mission, as defined by the ETP (2007), provides installation assets and services necessary to support our military forces in a cost effective, safe, sustainable, and environmentally safe manner. The RPILM CBM is focused on providing better information for strategic and tactical decisions, reducing the cost of business operations, improving stewardship and visibility of installations and environment assets, and supporting integration of DoD enterprise business operations (ETP 2007).

(5) Financial Management. The Financial Management CBM, as defined by the ETP (2007), is responsible for providing accurate and reliable financial information in support of the Planning, Programming, Budgeting, and Execution process to ensure adequate financial resources for warfighting mission requirements. The Financial Management Core Business Mission ensures that the DoD’s budget and financial expenditures support the national security objectives (ETP 2007).

c. Enterprise Transformation

DoD has identified and focused its transformation efforts on six strategic Business Enterprise Priorities, with the focal point being to make critical business information more visible and accessible. The Business Enterprise Priorities are Personnel Visibility, Acquisition Visibility, Common Supplier Engagement, Material Visibility, Real Property Accountability, and Financial Visibility. The plan for each priority details an overall strategy, key programs, and measurable program and business capability deliverables spread over the next several years (ETP, 2007).

(1) Personnel Visibility. Personnel Visibility (PV) is defined as having reliable information that provides visibility of military service members, civilian employees, military retirees, contractors in theater, and other U.S. personnel, across the full spectrum, during peacetime and war, through mobilization and demobilization, for deployment and redeployment, while assigned in a theater of operation, at home base, and into retirement (ETP, 2007). The ETP (2007) states the goal of PV is to provide accurate, timely and readily available personnel information (including data on military, civilians, contractors, and coalition resources supporting the operation) to decision makers.

(2) Acquisition Visibility. Acquisition Visibility (AV) is defined as achieving timely access to accurate, authoritative, and reliable information supporting acquisition oversight, accountability, and decision making throughout the DoD for effective and

efficient delivery of warfighter capabilities (ETP, 2007). The goal of Acquisition Visibility, as stated by the ETP (2007), is to bring transparency to critical information supporting full lifecycle management of the DoD's processes that deliver weapon systems and automated information systems.

(3) Common Supplier Engagement. Common Supplier Engagement (CSE) is defined as the alignment and integration of the policies, processes, data, technology and people to provide a consistent experience for suppliers and DoD stakeholders to ensure reliable and accurate delivery of acceptable goods and services to support the warfighter. The primary goal of CSE is to simplify and standardize the methods that DoD uses to interact with commercial and government suppliers (ETP, 2007).

(4) Material Visibility. Materiel Visibility (MV) is defined by the ETP (2007) as the ability to locate and account for materiel assets throughout their lifecycle and provide transaction visibility across logistics systems in support of the joint warfighting mission. The goal of Materiel Visibility is to provide users with timely and accurate information on the location, movement, status, and identity of unit equipment, materiel and supplies, in order to improve overall supply chain performance (ETP, 2007).

(5) Real Property Accountability. Real Property Accountability (RPA) is defined as providing the warfighter and CBMs access to near-real-time secure, accurate and reliable information on real property assets,

and environment, safety, and occupational health sustainability. The Real Property Accountability (RPA) goal is to provide the warfighter and other CBMs with continuous access to installations and environment information (ETP, 2007).

(6) Financial Visibility. Financial Visibility (FV) is defined as having immediate access to accurate and reliable financial information (planning, programming, budgeting, accounting, and cost information) in support of financial accountability throughout the DoD in support of warfighter missions. The goal for Financial Visibility is more efficient and effective decision making throughout the DoD and assisting in the DoD-wide effort to achieve financial auditability (ETP, 2007).

d. Component Transformation

This section of the ETP (2007) provides transformation updates for the following components: Department of the Army (DoA), Department of the Navy (DON), Department of the Air Force (DoAF), Defense Logistics Agency (DLA), United States Transportation Command (USTRANSCOM), Defense Finance and Accounting Service (DFAS), as well as covers enterprise-level transformation for the Military Health System (MHS).

e. Managing and Tracking Transformation

This section of the ETP (2007) provides information on two other components: the Defense Commissary Agency (DeCA) and the Defense Human Resources Activity (DHRA), and introduces the mission of each of the agencies,

followed by information about each of the certified systems, including a description of the systems, budget and the Business
Enterprise Priorities they support.

f. Information Technology Themes

- **Horizontal Integration Theme**

The ETP (2007) describes horizontal integration as the horizontal perspective to business that unites individual functions. It further discusses horizontal integration as a part of the DoD transformational effort that is being developed as a fully-integrated architecture using a cross-functional approach that enforces contribution and alignment from each functional element and integrates a set of business standards from end-to-end.

The five Core Business Missions (CBMs) are intended to be integrated horizontally across all business functions (e.g., planning, budgeting, IT, procurement, maintenance), as depicted below, to provide end-to-end support and mutual cross-coordination (ETP, 2007).

Figure 4. Core Business Missions (ETP, 2007)

For example, in Materiel Supply and Service Management (MSSM) CBM, the United States Transportation Command (USTRANSCOM) has been named as the Distribution Process Owner (DPO). As DPO, USTRANSCOM has responsibility that extends across the entire distribution process (not just transportation of people and material), based on a horizontal view of the entire supply chain and providing direct support to the Combatant Commands (COCOMs) (ETP, 2007).

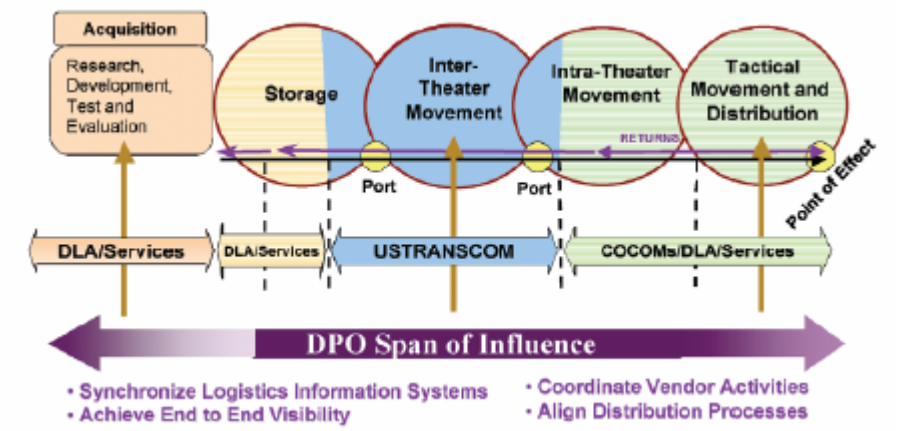

Figure 5. USTRANSCOM as DPO (ETP, 2007)

Another instance of horizontal focus can be seen in the Financial Visibility Business Enterprise Priorities. Financial Visibility crosses all CBM areas, and the Financial Management CBM (FM CBM) area maintains continuous coordination and collaboration with all other CBMs to ensure delivery of integrated enterprise capabilities (ETP, 2007).

- **Enterprise-level Solutions Theme**

As found in the ETP (2007), the focus of the defense transformation effort is on the process, data, and system elements enabling enterprise-wide information aggregation and system interoperability. Furthermore, capabilities that an enterprise-level solution should yield: (1) enterprise information visibility, (2) a single point of entry for business activity, (3) a common reference data for the DoD, or (4) a common enterprise wide transaction process (ETP, 2007). For example, Enterprise Resource Planning (ERP) implementation experts from the BTA team are working closely with all major ERP programs to ensure that standard implementation and configuration is achieved across DoD. As such, the components are migrating to Defense Integrated Military Human Resources System (DIMHRS), thereby creating a single pay and personnel system for the DoD; in order to provide an enterprise solution to facilitate the integration of military personnel and pay records.

- **Governance Theme**

A cultural shift in governance, as seen by the espoused commitment of DoD leadership, is meant to enable progress in business transformation (ETP, 2007). Schwartz (2007) defines IT governance as putting structure around how organizations align IT strategy with business strategy, ensuring that companies stay on track to achieve their strategies and goals. An approach to governance, tiered accountability, which is seen throughout the ETP (2007), focuses on the vertical aspects of the DoD organization, ensuring that the right people at the right level of the DoD organization assume the appropriate level of responsibility.

The figure below, developed by Failor (2007), is an example of an IT governance structure.

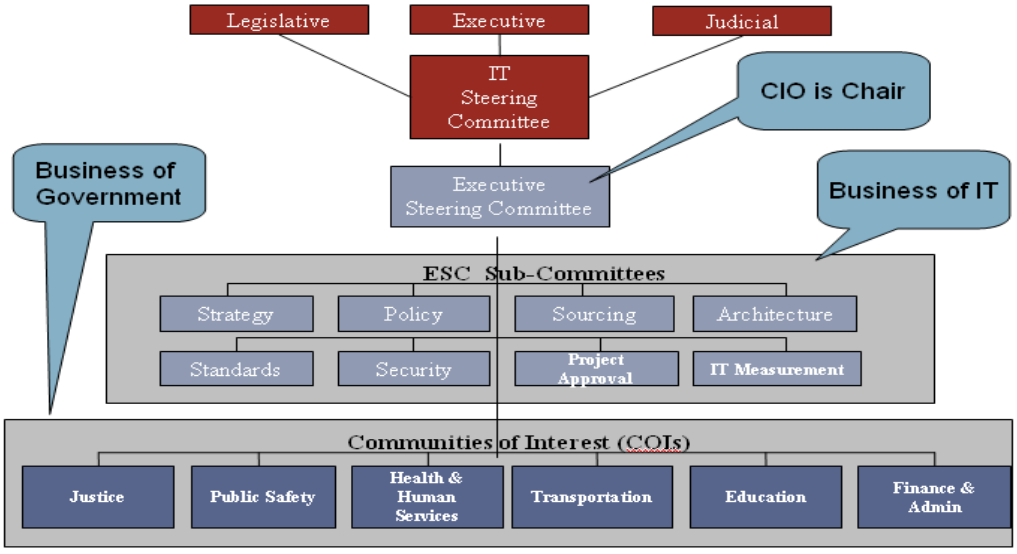

Figure 6. Sample Government: IT Governance Model (Failor, 2007)

The Common Supplier Engagement Business Enterprise Priority of the ETP (2007) uses a governance model to address stakeholder interest and align enterprise system development with the strategic goals of the DoD.

- **Information Visibility Theme**

Over the last several years, information visibility has been a clear theme of the Business Enterprise Priorities in the Enterprise Transition Plan. These priorities, which are focused extensively on the management and visibility of information, are appropriately centered on the needs of the enterprise level of the organization. Providing the decision makers access to timely, reliable, and accurate information, which encompasses information visibility, is a

fundamental capability of this theme. This focus requires more in the area of enterprise-wide data standards and business rules to enable information visibility for its stakeholders (ETP, 2007).

- **Net-Centric Data Strategy Theme**

The data strategy as described in the Enterprise Transition Plan is in alignment with the Net-Centric Data Strategy (2003) of the DoD which states that the foundation of the net-centric environment is the data that enables effective decisions. In this context, data implies all data assets such as system files, databases, documents, official electronic records, images, audio files, web sites, and data access services.

The ETP (2007), throughout all of the Business Enterprise Priorities, declares that the importance of establishing, documenting, and adhering to an enterprise-level procurement data strategy, associated data structures, and corresponding business rules is to support business transformation goals of the DoD.

The overarching objectives of the data strategy include: improving data quality, maximizing ability to leverage data from various sources-systems, improving visibility and monitoring quality of business processes, establishing and enforcing internal controls, improving interoperability and enforcing standards, improving ability to make strategic business decisions, and improving enterprise workload management (ETP, 2007).

The ETP (2007) describes the goal for the data strategy as establishing a data structure to be used in all department capabilities, identifying the minimum data needs

to be made available and shared among identified enterprise systems, functions, and components.

C. DEPARTMENT OF THE NAVY (DON)

Naval Power 21 is intended to serve as the Department of the Navy's vision statement guiding and supporting the naval transformation initiative. This vision encompasses the concepts of the selected DoN strategic documents, which are Sea Power 21 and the Department of the Navy Information Management/Information Technology Strategic Plan.

1. Sea Power 21 (SP 21)

The Chief of Naval Operations' (CNO) vision Sea Power 21 (SP 21) was introduced in Newport in 2002 as a coherent framework for the U.S. Navy to reorganize and focus on maritime capabilities to provide two fundamental outcomes for the nation: (1) Win the War on Terror; and (2) Provide Ready and Flexible Options for the President (Suttie, 2004). Sea Power 21 is the Navy's strategy to align, organize, integrate, and transform to meet future challenges. The CNO states it is global in scope, fully joint in execution, and dedicated to transformation. Three fundamental concepts are the foundation of SP 21: Sea Strike, Sea Shield, and Sea Basing. Sea Strike is the ability to project precise and persistent offensive power from the sea; Sea Shield extends defensive assurance throughout the world; and Sea Basing enhances operational independence and support for the joint force. Sea Strike, Sea Shield, and Sea Basing will be enabled by ForceNet, an overarching effort to integrate

warriors, sensors, networks, command and control, platforms, and weapons into a fully netted, combat force (Sea Power 21, 2002).

a. Information Technology Themes

- **Net-Centricity (ForceNet) Theme**

The concept of Net-Centricity, as previously discussed, is visible throughout Sea Power 21. As such, Sea Power 21 (2002) describes ForceNet, the link between Sea Strike, Sea Basing, and Sea Shield, as the operational construct and framework for naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. Furthermore, ForceNet provides the architecture to increase combat capabilities through alignment and integration of systems, functions, and missions.

- **Information Superiority Theme**

Joint Pub 3-13 defines information superiority as the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same.

Thus, the idea of information superiority is proliferated throughout Sea Power 21. Sea Strike and Sea Shield alike base information superiority as the foundation for their integrated operations. More specifically, under Sea Strike information gathering and management are the cornerstones of this concept (Sea Power 21, 2002).

- **Information Operations Theme**

The importance of information operations is stressed in Sea Power 21, more specifically in Sea Strike. Sea Strike describes how information operations will mature into a major warfare area, to include electronic warfare, psychological operations, computer network attack, computer network defense, operations security, and military deception. Information operations are viewed as a key role in controlling crisis escalation and preparing the battlefield for subsequent attack (Sea Power 21, 2002).

- **Information Sharing Theme**

Information sharing, as previously discussed, is a theme viewed as an integral part of Sea Power 21. Thus, Sea Shield discusses Homeland Defense and information sharing as the integration of forward-deployed naval forces with other military services, civil authorities, and intelligence and law-enforcement agencies. Interagency intelligence and communications reach-back systems are seen as a need while Sea Basing discusses the importance of international data-sharing networks.

2. DoN Information Management/Information Technology Strategic Plan

The Fiscal Year 2008-2009 Department of the Navy Information Management (IM) and Information Technology Strategic Plan, developed by the Chief Information Officer for the DoN, describes the DoN’s vision, mission, governing principles, goals, objectives, and key performance indicators for IM/IT to support the warfighter. It is driven

by, and aligned to, the overarching goals articulated by the Secretary of the Navy. The intent of this plan is to assist DoN Leadership by providing a vision that describes desired outcomes and identifies how they will be achieved and measured. This plan is also intended to help strengthen the alignment of subordinate commands with the DoN IM/IT goals and help clarify resource priorities. Furthermore, the plan is designed to provide the IM/IT workforce with an understanding of the direction of IM/IT in the DoN, and how their contributions support this vision (DoN IM/IT Strategic Plan, 2007).

a. Information Technology Themes

- **Net-Centric Theme**

The DoN IM/IT Strategic Plan calls for the planning, developing, implementing, operation, and sustainment of a global information infrastructure to provide secure, interoperable, and end-to-end connectivity to all Sailors, Marines, and civilians. The infrastructure's common architecture and technical standards allows for the Naval component of the DoD Global Information Grid (GIG) to maintain interoperability with joint forces, allied coalitions, and interagency partners (DoN IM/IT Strategic Plan, 2007).

- **Information Assurance Theme**

Information Assurance in the DoN IM/IT Strategic Plan looks at information resources, and critical infrastructures to provide assured information delivery, system and network access, and information protection. Solid information assurance concepts and principles are used throughout this

strategy to illustrate the method for protecting and providing secure systems, networks, and information. To that end, the focus is placed on establishing information assurance and system security protocols on all DoN networks in order to implement protection measures which protect, defend, and secure the mission-critical capabilities, and allow for available and secure information (DoN IM/IT Strategic Plan, 2007).

- **Seamless Business Infrastructure Theme**

Seamless business infrastructure is the direction that the DoN IM/IT Strategic Plan is focusing on, by way of a Navy and Marine Corps Portal strategy meant to provide the single sign-on gateway to the DoN's core enterprise applications, services, and processes. As such, this strategy is to align with DoD and Joint efforts with the objective being to eliminate legacy networks, servers, systems, applications, and duplicative data environments. Finally, by transforming proprietary and tightly coupled systems and applications into a set of enterprise services that emphasize loosely coupled (defined in Loosely Coupled (2008) as the friction-free linking enabled by web services (or any SOA). Loosely coupled services can be joined together on demand to create composite services, or disassembled just as easily into their functional components.) systems and processes; these enterprise services are intended to provide seamless connectivity to mission critical information leveraged across the DoN (DoN IM/IT Strategic Plan, 2007).

- **Knowledge Superiority Theme**

Through integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force; ForceNet provides secure, assured, accurate, and timely information to the warfighter. The DoN IM/IT Strategic Plan assumes that by enabling the information value chain of identity management, information assurance, authoritative data bases, fast and accurate search, and content management will positively impact the management of knowledge, leading to knowledge superiority. Furthermore, this strategy plans for the rapid exchange of all source knowledge for the effective employment of the DoN's intelligence capability, battlefield awareness insight, and weapons capabilities. Similarly, the plan emphasizes a seamless transfer of knowledge between people and applications in designing and deploying future support processes. The DoN plans to move from a culture that rewards the retention of data and information to one that rewards effective knowledge stewardship (DoN IM/IT Strategic Plan, 2007).

- **Align IT Investments with Warfighting Strategy Theme**

The DoN IM/IT Strategic Plan directs the selection of efficient and effective IM/IT investments based on validated user requirements. These investments align with the strategic priorities established in governmental, DoD, and DoN guidance, which align with the DoD Global Information Grid (GIG) strategy and the Business Transformation Agency guidance allowing for interoperability within the Joint and Coalition environments. In order to provide the ability to

quantify the return on investment and total cost of ownership in a standard manner across all programs the strategy suggests transparent investment costs and standardized evaluation criteria (DoN IM/IT Strategic Plan, 2007).

D. UNITED STATES MARINE CORPS (USMC)

The Navy and Marine Corps have defined their respective Service strategies in Sea Power 21 and Marine Corps Strategy 21. These documents define their advancement into the future as a part of the overall joint force, and allows for the focus of efforts and resources within each Service through the implementation of the key concepts found within each strategy (Naval Power 21, 2002). The USMC selected documents for review are the Marine Corps Strategy 21, Commandant's Planning Guidance, and the USMC Concepts and Programs.

1. Marine Corps Strategy 21

Marine Corps Strategy 21, published by Headquarters Marine Corps, is intended to provide the vision, goals, and aims to support the development of future combat capabilities. Additionally, it is intended to support development of advanced strategic agility, operational reach and tactical flexibility by enabling joint, allied, and coalition operations (Naval Power 21, 2002). Furthermore, the plan provides strategic guidance to active and reserve Marines, Sailors, and civilian personnel with the goal of capitalizing on innovation, experimentation, and technology. (Marine Corps Strategy 21, 2000)

a. Information Technology Themes

- **Net-Centric Theme**

Participating in a Net-Centric environment within the Marine Corps is seen as one of the goals in the Marine Corps Strategy 21. Furthermore, the intent is to capitalize on innovation, experimentation, and technology in order to prepare Marine Forces to succeed in the 21st century. Similarly, the Marine Corps intends to focus on network operational communications, information, and intelligence systems with joint and allied forces and provide a global access capability to domestic and international information resources (Marine Corps Strategy 21, 2000).

2. Commandant's Planning Guidance

Each Commandant of the Marine Corps publishes a Commandant's Planning Guidance. The guidance describes the Commandant's number one priority and discusses areas of focus with that priority in mind. The document reviewed for this research is the 34th Commandant of the Marine Corps, General Conway's, Commandant's Planning Guidance

a. Information Technology Themes

- **None**

3. USMC Concepts and Programs

Concepts and Programs (2007), (formerly called Concepts & Issues), is a publication produced annually by the Programs and Resources Department of the Marine Corps. Concepts and Programs articulates the modernization

requirements of the United States Marine Corps, and presents an overview of current plans to give the Marines, in pursuit of America's national security the best warfighting tools available. Concepts and Programs offers a broad perspective across the Marine Corps that includes a description of the conceptual view of warfighting, an overview of the operations of the past year, and an examination of the specific programs that will provide the Marines technologically superior weapons platforms, systems, and equipment.

a. Information Technology Themes

- **Net-Centric Theme**

Concepts and Programs (2005) discuss 21st century Marines through Net-Centric capabilities. One capability discussed is Distributed Operations (DO), an approach that is applicable at both the operational and tactical levels of war, by which a commander alternately disperses and concentrates networked forces to define and shape the battlespace. Additionally, DO serve as a bridge to expanded operations with other networked joint forces, a method to improve situational awareness, which includes real time and high fidelity data from dispersed teams, improving the vertical transmission of information.

- **Information Operations (IO) Theme**

Another concept of the 21st century Marine discussed in Concepts and Programs is Information Operations. Information Operations at all levels requires careful planning and integration. However, from the Marine Corps perspective, IO is not a warfighting function in its own right; it is an

integrating concept that facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection. Thus, it is suggested that the focus of Marine Corps IO be based on the information-oriented activities that best support the tailored application of combat power and the joint force commander's needs (Concepts and Programs, 2005).

E. SUMMARY

The following four compilation figures compare IT themes identified throughout this literature review.

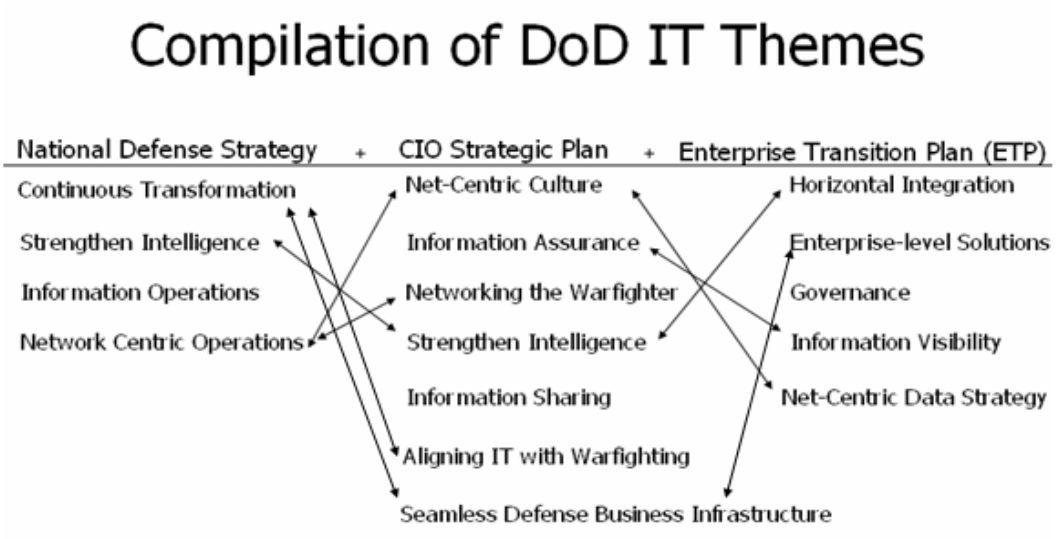

Figure 7. Compilation of DoD IT Themes

Figure 7 is a compilation of themes found within the specific DoD strategic documents with similar themes connected with an arrow. The connected themes will be combined and identified by one theme in the total compilation figure.

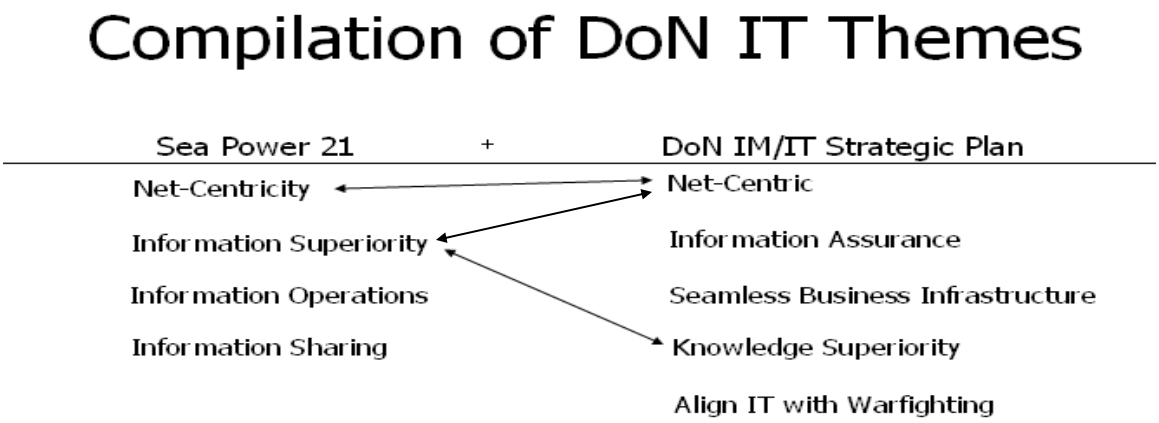

Figure 8. Compilation of DoN IT Themes

Figure 8 is a compilation of themes found within the specific DoN strategic documents with similar themes connected with an arrow. The connected themes will be combined and identified by one theme in the total compilation figure.

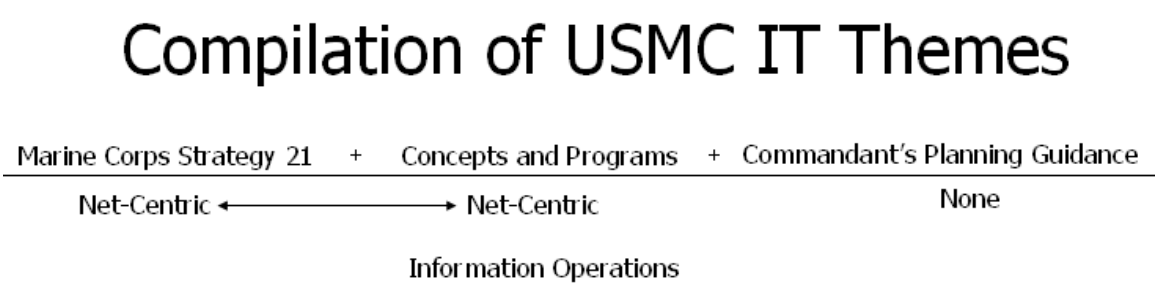

Figure 9. Compilation of USMC IT Themes

Figure 9 is a compilation of themes found within the specific USMC strategic documents with similar themes connected with an arrow. The connected themes will be combined and identified by one theme in the total compilation figure.

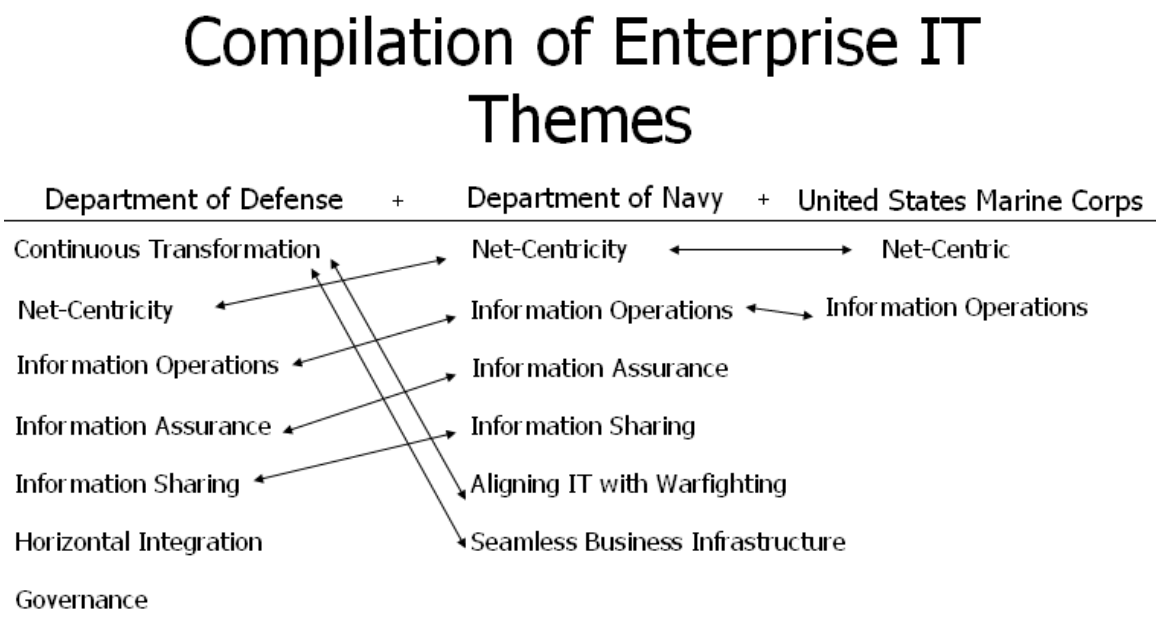

Figure 10. Compilation of Enterprise IT Themes

Figure 10 is a complete compilation of themes found within all reviewed strategic documents of this chapter with similar themes connected with an arrow. The connected themes will be combined and identified by one theme in the summarization table.

Summarization of Enterprise IT Themes

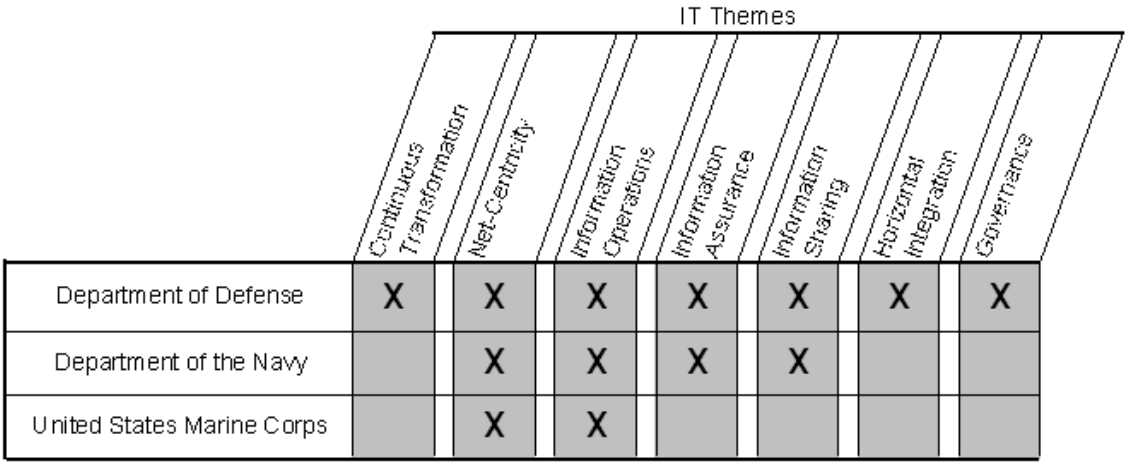

Table 1. Summarization of IT Themes

Table 1 delineates the IT themes across the enterprise (DoD, DoN, USMC) and the commonality or non-commonality between the organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CURRENT ACQUISITION PROGRAMS REVIEW

A. INTRODUCTION

This chapter summarizes six information technologies (IT) related acquisition programs being developed and/or sponsored by Department of Defense (DoD), Department of the Navy (DoN), and U.S. Marine Corps (USMC) strategic and operational planners. At least one business system and one tactical system are specifically addressed for each enterprise.

B. DEPARTMENT OF DEFENSE PROGRAMS

This section summarizes the following two DoD acquisition programs: the Defense Integrated Military Human Resources System (DIMHRS), a business system, and the Joint Command and Control tactical system (JC2).

1. Defense Integrated Military Human Resources System (DIMHRS)

a. Background

Since early days of data automation, each military Service has developed their own unique business systems to manage complex personnel resources. Although there are inter-Service differences in mission, programs, and legislative priorities, multiple Service data automation and IT redundancies are not reflective of the defense mandate towards jointness, flexibility, accuracy, speed and security; all delivered in the context of on-going, complex

and global operations. DoD has a multitude of unique personnel systems, many of which support other Service unique systems (BTA, 2007).

In 1992, the military personnel Information Management (IM)/Business Process Reengineering (BPR) program was initiated to address some of the above mentioned issues. The overarching goal is to support and enable the joint operations mission, particularly in terms of a marked focus on supporting warfighters. Additional goals include promoting and maintaining responsive military personnel management and ensuring that accurate and timely data are available throughout applicable strategic, operational and tactical oversight levels (DIMHRS ORD, 2005).

The IM/BPR program addresses critical problems highlighted after Gulf War I. For example, how best to integrate Active, Guard, and Reserve data bases and personnel and pay functionality, including efforts to streamline and improve automated support to mobilization and deployment venues. Intentions include standardized data reflecting core requirements of Combatant Commands (COCOM), Military Services, the Office of the Secretary of Defense (OSD), and other Federal agencies (DIMHRS ORD, 2005).

In 1995, a Defense Science Board (DSB) Task Force on Military Personnel Information Management was established to advise the Secretary of Defense on the best strategy to support military personnel and pay functions. The Task Force concluded "…that the present situation, in which the Services develop and maintain multiple Service-unique military personnel and pay systems, has led to significant functional shortcomings (particularly in the joint arena) and excessive costs for system development and maintenance

for the Department of Defense" (DIMHRS ORD, 2005). Their recommendation was, "…the Department should move to a single all-Service and all-component, fully integrated personnel and pay system, with common core software…" (DIMHRS ORD, 2005).

b. Mission Need

On October 6, 1997 the Mission Needs Statement (MNS) for DIMHRS was provided to the Secretaries of the Military Departments and was subsequently approved on February 24, 1998. As shown in Figure 2, the MNS listed the following five major problem areas needing resolution:

- COCOMS did not have access to accurate or timely data on personnel needed to assess operational capabilities.
- OSD and joint managers and other users of data were hindered by the lack of standard data definitions and could not make necessary comparisons across Services.
- Reservists who were called up were sometimes "lost" in the system impacting their pay, their credit for service, and their benefits.
- Active personnel (and reservists) were not tracked into and within a theater of operations.
- Linkages between the personnel and pay functions were different among the Services resulting in multiple data entry, complex system maintenance, reconciliation workload, and pay discrepancies. (DIMHRS ORD, 2005)

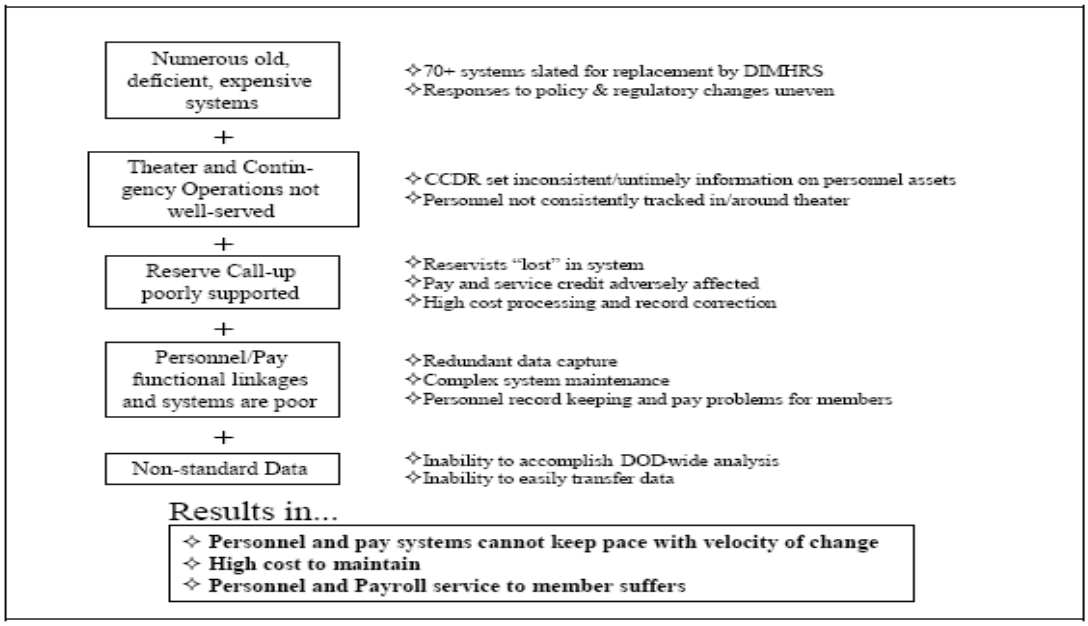

Figure 11. Major Environmental Deficiencies (DIMHRS ORD, 2005)

c. Concept of Operations

- DIMHRS was created to provide the individual Service member, DoD civilian, and contractor, personnel and pay support throughout the member's military/civilian career, including being the single, authoritative source of data concerning individual affiliation with the DoD.
- DIMHRS will support the personnel and pay needs of commanders throughout the operational forces. Identifying the required personnel (i.e., military service member, civilian, or contractor), their status, and organization encompass the minimum basic information required by commanders.
- DIMHRS will employ standard business processes to the maximum extent possible generating standardized

data. It will provide common functionality, common information and data exchange, and associated common core databases across the Department, again supplemented by Service specific needs.

- DIMHRS will reduce the number of intermediate nodes between source data input and headquarters database management and applications within the operational architecture.
- DIMHRS will provide a flexible environment enabling maximum use of emerging technologies. As Services modify force structure, DIMHRS is to provide a flexible system designed to meet any relevant challenges. (DIMHRS ORD, 2005)

d. Technical Capabilities Required

The functional base-line starting point of DIMHRS consists of the core business processes common to all Service Components. The processes that support the functional base-line will be reengineered and combined with solutions to the deficiencies noted in the mission needs statement, and used as the starting point for DIMHRS design. Functional requirements will be identified by Service Component stakeholders in order to fully support this integrated military personnel and pay system. DIMHRS is to meet or exceed existing service component systems' functionality, except where that functionality has already been replaced by reengineering processes. DIMHRS will not reuse data that is archived by legacy systems prior to its implementation. It will however, migrate active data from legacy systems as they are replaced. DIMHRS will also

provide a capability to query archived data if DIMHRS is replacing the system that contains the query capability. (DIMHRS ORD, 2005)

DIMHRS will support approximately 2.6 million military personnel of all Services and their Components at the Services' personnel support activities. It will collect, store, pass, process, and report personnel and pay data for these personnel. In addition, DIMHRS will provide the capability to collect, process, and report appropriate data on DoD-sponsored civilians and designated foreign military personnel deployed to or in a theater of operations as required during specified contingency, wartime and non-combatant evacuation operations. In support of this capacity, the system will interface with the Defense Civilian Personnel Data System (DCPDS). It will maintain personnel information on approximately 3 million retirees and survivor personnel; however, the Defense Retiree and Annuitant Pay System (DRAS) will continue to provide pay support to this population. Information requirements will be identified early so that DIMHRS and DRAS can be responsive to changes in interface requirements. DIMHRS will provide the information requirements necessary to support the needs of the Unified Combatant Commanders as established in "CINC 129 Information Requirements dated 29 November 1999." (DIMHRS ORD, 2005)

The DIMHRS program includes software application development efforts. The DIMHRS Joint Program Management Office (JPMO) is part of the Program Executive Office for Information and Technology, and is in charge of development, including responsibility for defining the infrastructure required to support the system. The initial operating

capability (IOC) of DIMHRS will be fielded on existing Service Component owned computer hardware as well as using Service Components communications infrastructure. Intra-operability (e.g., inside Service) needs between the DIMHRS IOC and host Service legacy personnel and pay systems will be supported by DIMHRS open systems (The DoD's Open Systems Joint Task Force (OSJTF) (2008) defines an open system as: A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability) design standards to ensure Service systems can exchange data and use personnel asset visibility information. In addition, DIMHRS will interoperate with authorized external systems by providing them with the personnel and pay data they require. (DIMHRS ORD, 2005)

DIMHRS is designed to be a knowledge based system that incorporates policy rules to ensure users are not required to make policy determinations. Input and help capabilities, and data integrity edits are to ensure data complies with defined business rules. Processes and systems will continue to support all current functions unless those functions are eliminated during process reengineering. This means that interfaces to all legacy systems not replaced will be built and/or maintained. (DIMHRS ORD, 2005)

e. System Description

DIMHRS is a joint personnel and pay system that is intended to replace about 80 legacy personnel systems and provide personnel and pay services for all DoD military personnel. DIMHRS Operational Requirements Document (2005) suggests that the functional architecture reflect core business processes used in all the Services, e.g., generating assignment orders, providing casualty assistance, and promoting enlisted and officer personnel. Service-specific needs can be supplemented such as changes in force structure. The core system will collect, store, transmit, process, and report personnel and pay data for all DoD active duty, Reserve, National Guard, and retired military personnel. Service-specific functionality can be provided by DIMHRS for any pay and personnel management processes previously supported by Service legacy systems. (Information Technology, 2002)

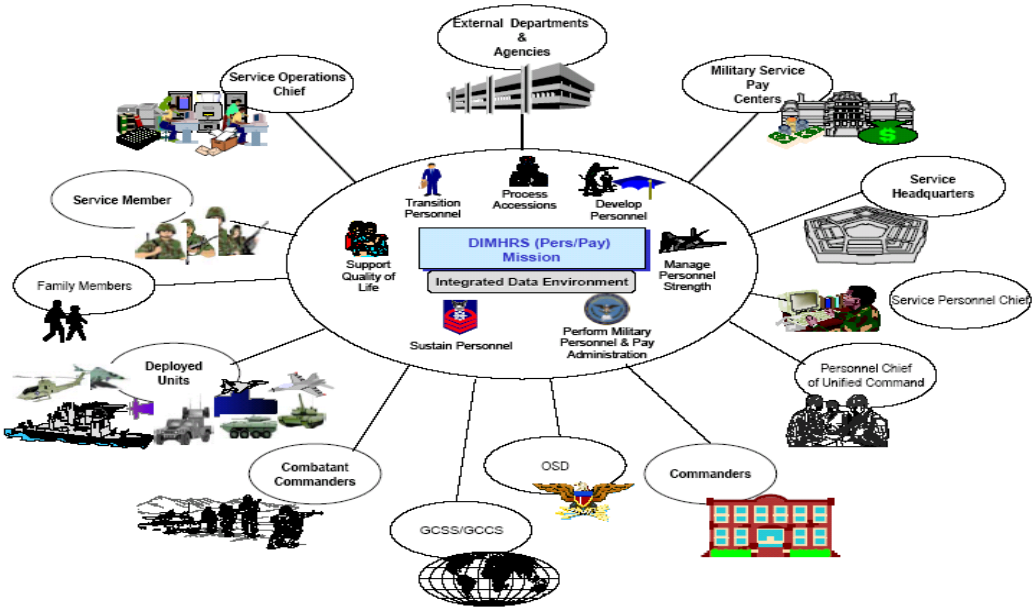

Figure 12. High-Level Operational Concept Graphic (DIMHRS ORD, 2005)

f. Desired End State

The overall goal for DIMHRS is to provide a fully integrated military personnel and pay system for all DoD military Service Components (DIMHRS Project Overview, 2004). DIMHRS is consistent with the DoD strategy of continuous transformation as an enterprise-wide solution for how the DoD accesses and manages critical member information. Common knowledge indicates that commanders and directors are well-served when complex technology answers their crucial questions of: Where are my people? What are their skill sets? and, How can technology be further used to assist decision makers? (ETP, 2007)

2. Joint Command and Control (JC2)

a. Background

Since September 11, 2001, the US government has focused on protecting the Nation from external and internal terrorist attacks. To that end, the need to extend command and control interoperability to support the exchange of secure information with allied, coalition and non-DoD partners has risen dramatically. Thus the Global Command and Control System (GCCS) and the DoD Command, Control, Communications and Intelligence (C4I) system (previously comprised of joint and Service variations) is evolving into a single joint command and control architecture focusing on capabilities vice Service specific functions. For example, the capability to share access to data sources produced from Service, Agency, and theater-of-operations via the Global Information Grid (GIG) infrastructure. These capabilities encompass the following mission capability packages and sets of software applications supporting each respective joint mission capability area: Force Planning, Deployment, Sustainment, Readiness, Intelligence and Situational Awareness; Force Employment - Air/Space Operations; Force Employment - Joint Fires/Maneuver, and Force Protection. (JC2 ORD, 2002)

b. Mission Need

According to the JC2 ORD (2002), the GCCS does not fully support the warfighters, policy makers, and support organizations joint command and control requirements within wartime and peacetime environments. The existing system focuses on vertical information exchanges and does not

address horizontal information flows among joint force components. Information flow difficulties are further complicated in terms of connectivity requirements with allied, coalition, and non-DoD partners. Lack of joint interoperability between legacy, service unique command and control systems precludes a reliable, timely and accurate exchange of information. Lack of a common joint data model restricts search and retrieval capabilities as users generate excessive transaction costs sorting through irrelevant or duplicative data. Obviously, mastering complex data interchange across joint, allied, and coalition global operations is deemed crucial for maintaining and ensuring information dominance to accomplish national security objectives. (JC2 ORD, 2002)

c. Concept of Operations

JC2 is projected to provide allied and coalition partners secure access to required mission capabilities intended to meet the dynamic information needs of warfighters. Vertical and horizontal information exchange will be met through mission capability packages allowing commanders and their staffs to analyze shared data, project requirements, and make time-sensitive decisions. (JC2 ORD, 2002)

The JC2 will provide commanders various mission capability areas to assist in decision making, to increase battlespace awareness, and to accommodate interactive information exchange. For example:

- **Force Planning/Deployment/Sustainment.** Deliberate and crisis action planning; deployment/redeployment planning and execution, identification of forces and

total assets, force movement; provision of personnel, logistic, and other support required to execute military operations until assigned missions are accomplished.

- **Force Readiness.** Assessing US forces' ability to undertake wartime and current missions.
- **Intelligence.** Joint Intelligence Preparation of the Battlefield (JIPB), targeting, Intelligence, Surveillance, and Reconnaissance (ISR) management.
- **Situational Awareness.** Fused battlespace awareness tailored to provide current and projected disposition of hostile, neutral, and friendly forces through near real time (NRT)/real time (RT) sensor data and shared data from national and theater sources.
- **Force Employment - Air and Space Operations.** Transition from force-level planning to execution including command and control activities associated with management of air and space assets.
- **Force Employment - Joint Fires/Maneuver.** Transition from force-level planning to execution including command and control activities associated with management of joint fires/maneuver assets.
- **Force Protection.** Warning and planning required to minimize vulnerability of joint, allied, coalition, and US organizations from enemy/terrorist threats. Activities include theater ballistic missile defense, Homeland Defense (HLD)/Homeland Security (HLS), consequence management, and related crisis response operations. (JC2 ORD, 2002)

d. Technical Capabilities Required

JC2's required capabilities are designed to counter or mitigate shortfalls identified in the Mission Needs section through the following:

- **JC2 Mission Capability Packages (MCP).** JC2 MCPs are sets of software applications supporting each respective joint mission capability area enabling vertical and horizontal information exchange. (JC2 ORD, 2002)
- **Cross-functional Services.** Through the use of cross-functions, sets of software applications providing common functionalities supporting two or more MCPs, JC2 integrates collaborative capabilities, such as audio, video, video teleconferencing (VTC), whiteboard, text chat, and application sharing. Furthermore, the cross-functional service of Multi-level Security (MLS) supports simultaneous operation at different security levels, compartments, and categories to include: TS and below, NATO releasable, allied releasable, coalition releasable, SIOP, SAP, and SCI. JC2 must allow information to be pushed/pulled from multiple data sources at different security levels from a single thin client. Training includes computer-based (on-line & downloadable) mission and system administration training capabilities. Office Automation provides advanced word processing, graphic presentation, spreadsheet analysis, and language translation tools. Messaging provides advanced capabilities to include commercial electronic mail/messaging,

Defense Message System (DMS) User Agent/client, and Automated Message Handling System (AMHS) services. Information Assurance (IA) provides advanced capabilities to protect JC2 and shared Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) information from the full range of potential cyber threats by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. IA provides for restoration of systems by incorporating protection, detection, and response capabilities. (JC2 ORD, 2002)

- **Shared Data Sources.** Shared data sources are the databases produced by the Services, Agencies, and theater-of-operations essential to the Joint Chiefs of Staff and JFCs' ability to plan, execute, and assess joint, allied, and coalition operations. Using MCP applications, JC2 users will have access to multiple time-sensitive data sources; data sources include force-level planning, force readiness, situational awareness tracks, force protection, Joint Intelligence Preparation of the Battlefield (JIPB), targeting, ISR management, and geo-spatial databases. The JC2 architecture will be robust and scalable to integrate additional data sources as required (e.g., HLD/HLS). (JC2 ORD, 2002)
- **Net-Centric Enterprise Services (NCES).** JC2 MCPs will utilize infrastructure services and common data strategy to be provided by the NCES. Major NCES components include the Common Operating Environment (COE), Shared Data Environment (SHADE), Information

Dissemination Management (IDM), and Applications Service Management (ASM). JC2 will leverage COE infrastructure to enable transformation from a heavy client/server to a thin client/web-enabled environment.

SHADE will provide common data representations supporting information sharing and improving the warfighters' ability to pull current information from shared data sources using web-enabled applications. IDM will enable intelligent search and retrieval through common cataloging, enterprise-wide search capabilities, and secure information delivery mechanisms. ASM will support systems administration and management of the distributed Global Information Grid (GIG) functionality within NCES. (JC2 ORD, 2002)

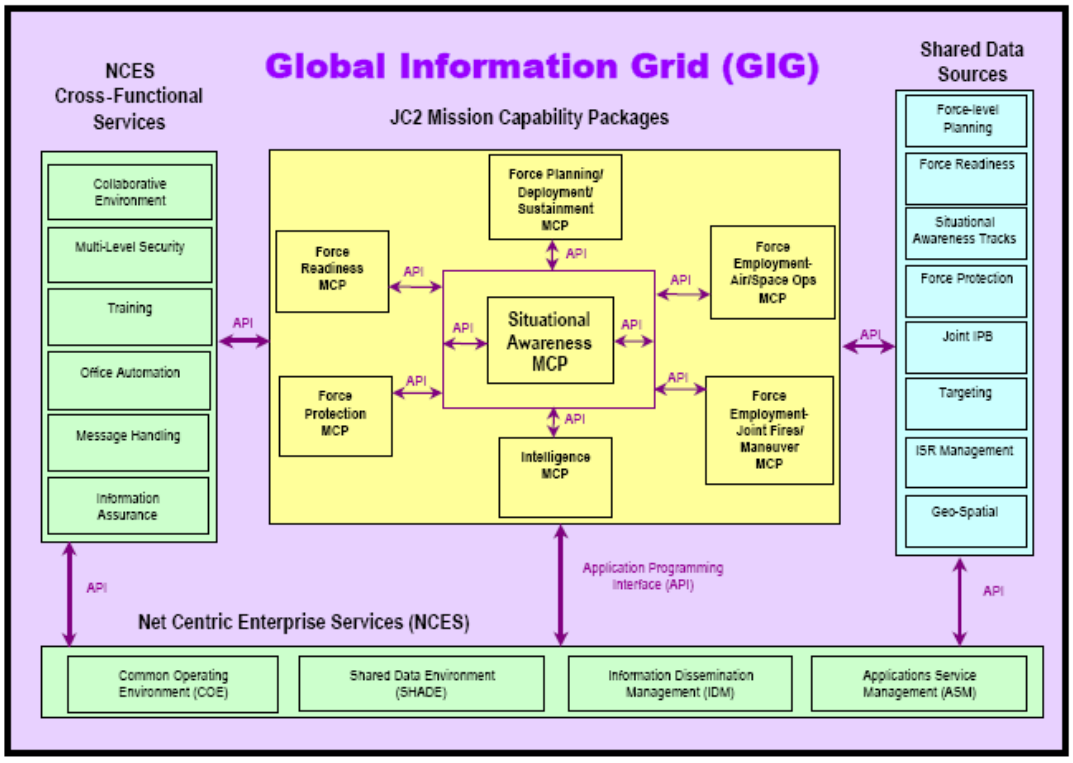

Figure 13. JC2 System Interface Description, Intrasystem Perspective (JC2 ORD, 2002)

e. System Description

The Joint Command and Control (JC2) capability will be the DoD principle command and control system. Furthermore, the JC2 will consist of the trained personnel, mission capability packages, and spell (GIG) infrastructure required to plan, execute, and assess joint, allied, and coalition operations. JC2 will operate in garrison and deployed local area network environments and will support simultaneous operations at different security levels, compartments and categories including: Top Secret and below, NATO releasable, allied releasable, coalition releasable, Single Integrated Operation Plan (SIOP), Special Access

Program (SAP), and Sensitive Compartmented Information (SCI). The purpose is to enable the Joint Chiefs of Staff and Joint Force Commanders (JFC) to administer and operate with greater speed, efficiency and interoperability, and reduced logistics support requirements. (JC2 ORD, 2002)

JC2 will support secure communications and provide reachback capabilities to shared data sources produced by Service, Agency, and theater-of-operations by using Defense Information System Network (DISN) services, Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Teleport, and Joint Worldwide Intelligence Communications System (JWICS) and commercial networks. (JC2 ORD, 2002)

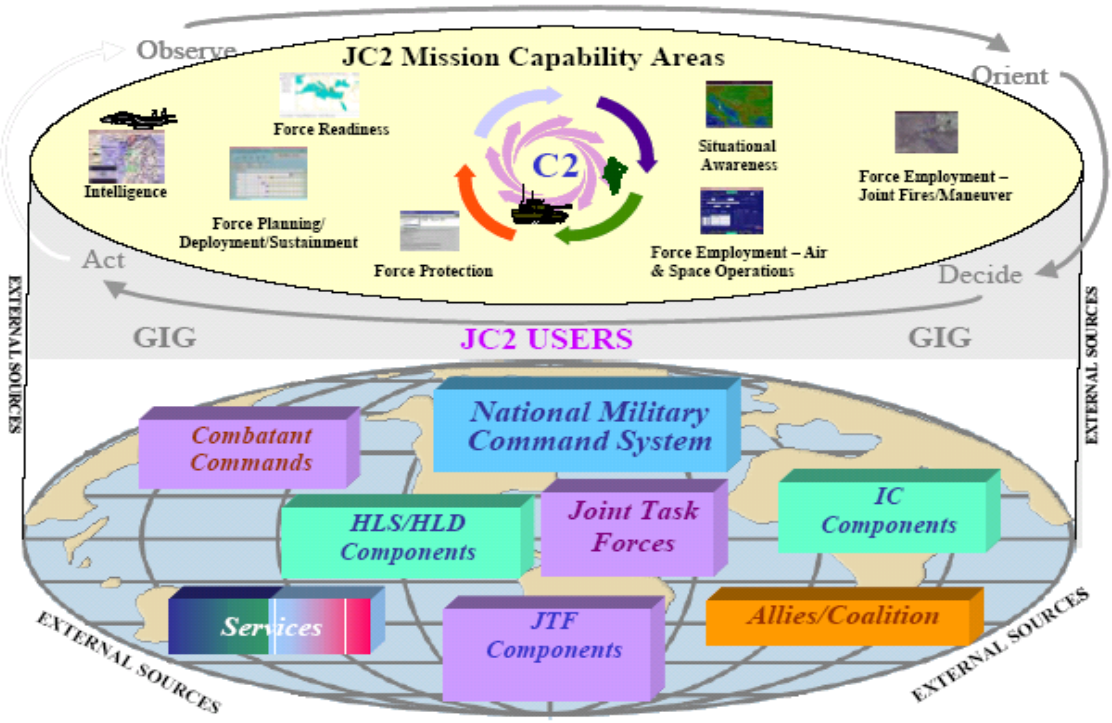

Figure 14. JC2 High-Level Operational Concept Graphic (JC2 ORD, 2002)

f. Desired End State

Joint force commanders may use JC2 to accomplish force-level planning, execution, and assessment activities in support of joint, allied, and coalition operations. Commanders often require a secure, collaborative, web-enabled, and tailorable command and control architecture that enhances the decision making process, including vertical/horizontal interoperability. (JC2 ORD, 2002)

C. DEPARTMENT OF THE NAVY PROGRAMS

This section summarizes the following major acquisition programs for the DoN: Navy Enterprise Resource Planning (ERP) program, a business initiative; and the Global Command & Control System - Maritime (GCCS-M), a tactical system.

1. Navy Enterprise Resource Planning (ERP)

a. Background

The Navy is looking for a fully integrated means for planning, acquiring, and managing Naval personnel, financial and material resources, and is implementing an Enterprise Resource Planning (ERP) program. The task includes providing a standard set of tools to Naval organizations that will facilitate business process reengineering efforts, including providing interoperable data elements for acquisition, financial, and logistics operations. As a goal stated in Joint Vision 2020, the Navy ERP looks to provide the joint forces the right personnel, equipment, and supplies in the right place, at the right

time, and in the right quantity, across the full range of military operations. (Navy ERP ORD, 2004)

b. Mission Need

The existing collection of “stovepiped” defense resource management systems places limitations on operational and support commanders to rapidly respond to dynamic operational requirements and redirect assets as needed. Many of the systems and processes currently in use were designed to support functional organizations and logistics, maintenance and support practices developed in the 1960s. These systems were not designed to support current logistics requirements, particularly during warfare operations. The Navy ERP ORD (2004) identifies shortcomings of existing systems accordingly:

- Information systems are not well integrated with local support organizations resulting in data integrity problems adversely impacting mission accomplishment and generating inefficient transaction costs.
- Systems are characterized by non-standard human to computer interfaces (i.e. forcing the user to learn the intricacies of the computer system vice the specifics of the process), complex processes, non-standard data with high error rates and significant delays in information exchange.
- The processes associated with current systems often deal with high volume; individual entries; paper-based forms; high transaction rates; and multiple levels of authorization, approval, or audit.

- Legacy systems support specific functional processes leading to non-interoperable “stovepiped” systems comprised of many interfaces expensive to develop and maintain.
- Current system software was built for specific hardware and cannot be easily and economically transferred to more modern hardware.
- The systems do not make use of labor saving technologies or best practices.
- Current systems do not provide real or near real time exchange of information.

c. Concept of Operations

The primary objective of the Navy ERP Program is to act as a vehicle for transforming key acquisition, logistics, and financial business activities into an integrated network of decision-making processes and business activities. (Navy ERP ORD, 2004) To that end the Navy ERP is designed to:

- Facilitate an End-to-End solution for receiving requests for resources and for processing those requests to fulfillment.
- Replace the segregated software systems currently used for financial management, inventory management and industrial operations, with a single integrated software program with modules that support organization functions.
- Enable managers and line personnel to rapidly determine operating force logistics needs and

respond rapidly to requirements through the system's integrated database, visibility and status of transactions.

- Reduce the overall cost to the Navy by applying proven industry best practices and processes and replacing legacy IT systems. (Navy ERP ORD, 2004)

d. Technical Capabilities Required

The Navy ERP Program is pursuing a COTS suite of pre-engineered, ready-to-implement, integrated application models. These models are to deliver process improvements and performance by standardizing processes and information requirements. Integrated processes are to be accessed through a single data source that provides consistent, up-to-date information to all the business functions thereby reducing or eliminating time-consuming system reconciliation. (Navy ERP ORD, 2004)

The target architecture of the Navy ERP Program is the Web-Enabled Navy (WEN) Architecture, which is an ERP web services architecture based on industry best practices leveraging powerful new technology to move and share data (CHIPS, 2003). These services are accessible through the Navy Enterprise Portal (NEP), which was developed to provide the enterprise infrastructure for accessing web services through a common user interface (CHIPS, 2003). The chosen ERP software is planned to be customizable, scalable and highly suited for many types and sizes of organizations with the ability to ensure prompt, quality feedback to all entities within the enterprise. The proposed architecture is comprised of application and database servers. The

application servers contain the software and database servers handle document updates and master file databases. (Navy ERP ORD, 2004)

The functions of Template 1.0 (Finance, Program Management, I-Level Maintenance, Plant Supply, Work Force Management, Travel Management and Wholesale Supply) will employ the proposed system architecture. Functionality within the Navy ERP program scope will be obtained from licensed COTS providers or from interfaces to viable legacy systems as required. The Navy ERP Financial functional interface with DoD Financial on the GIG and will include an interface to receive electronic invoices from the Wide Area Work Flow (WAWF) system and authorize electronic payments related to those invoices based on three-way matching inside ERP. Travel Management employs an interface between the Finance function and Defense Travel System (DTS). Work Force Management functions will interface with the following:

- Defense Civilian Personnel Data System (DCPDS) via the OCHR Navy Data Mart
- Defense Civilian Pay System (DCPS)
- Manpower and Personnel Enterprise Database (EDB), which will migrate to the Defense Integrated Military Human Resources System (DIMHRS). (Navy ERP ORD, 2004)

The Navy ERP Program will ultimately interface with both ashore and afloat commands. Within continental United States (CONUS), the Navy ERP Program will rely on the Navy and Marine Corps Intranet (NMCI) infrastructure for data transport and security. Commands located outside the continental United States (OCONUS) will gain access through the Base-Level Information Infrastructure (BLII), assets

including wire, fiber optic, and other connected voice, video and data resources such as servers, routers and telephone switches (BLII, 2008). The Navy ERP Program will provide accessibility and availability of information to authorized entities and to all applicable, authorized systems to include Joint interfaces located on the GIG. The exchange of information with Joint systems on the GIG may include classified systems extracting unclassified information. (Navy ERP ORD, 2004)

e. System Description

The Navy ERP Program will use an evolutionary or incremental acquisition strategy to deliver usable portions of capability. Configured increments (templates) will provide a logical set of functionality to predetermined deployment sites. Each future increment will build upon the accomplishments of previous increments and minimize major user interface changes. The initial template (Template 1.0) addresses finance, program management, intermediate level maintenance, plant/wholesale supply, travel management and workforce management functions across the Naval maritime, aviation, nuclear, sustainment, and supply business areas.

These seven functions document the required business functions for the Navy ERP Program. The Navy ERP Program will provide the same level of functional readiness and technical performance in peacetime, wartime, and during contingency operations. The Navy ERP ORD (2004) provides a detailed description of the individual functions described as follows:

(1) Finance. Functions include Billing, Asset Accounting, Revenue and Cost Controlling, Period End Close, Financial Reporting, and Financial Accounting. Wide Area Work Flow (WAWF) will also interface with the Finance function to maintain the paperless contracting concept. Financial functionality will provide the ability to monitor:

- Financial Statement Cycle Time (Internal and External Reporting)
- Funding Receipt to Acceptance Cycle Time
- Track funds and financial documents from all sources
- Reports of funds expended versus funds allocated
- Vendor Pay Cycle Time
- Funds Lost to Late Invoices per Year
- Funds Lost to Problem Disbursements per Year
- Funds Lost Due to Interest Payments on Late Vendor Payments Per Year

(2) Program Management. Program Management (PM) functions include project initiation, tracking and modifications, including the following capabilities:

- Prepare a cost estimate, reducing the turnaround time to create, schedule, resource load, and calculate (planning) costs for a multi-year project
- Prepare impact statements due to a potential budget mark, reducing turnaround time to provide a trade-off analysis and cost impact for a project already in execution
- Reduce the turnaround time to create and submit a project report

- Reduce the project manager’s turnaround time to submit a project cost plan to support budget formulation and associated budget exhibits
- Reduce Cycle Time Required to Create Monthly Reports;
- Generate work breakdown structures (WBS)
- Track program cost and schedule.

(3) Procurement. Procurement functions include Purchase Card, Electronic Procurement for consumables, Large Contract and Simplified Acquisition awards, Repair Services with Commercial, Navy Depots and other Services and Purchase Orders for Training Requests and Travel Orders. Goods receipt and invoice verification are also performed Procurement functionality is meant to enable monitoring and management of:

- Vendor Evaluations (timely delivery, quality assurance, quotation analysis, Procurement Lead time),
- Procurement Administrative Lead Time (PALT) for Simplified Acquisition,
- Cost vs. Plan,
- Commitment (Requisition) and Obligation Aging Reports
- Administrative Lead Time to place contract for a wholesale requirement.

(4) I-Level Maintenance. Functions include Intermediate-Level Maintenance Management, maintenance planning, preparing task lists, defining breakdown and

planned maintenance processes, Quality Management, Calibration management and master technical data management. These capabilities are designed to improve:

- On-Time Performance
- Total Direct Cost and Forecasting Accuracy
- Direct Cost Per Job and Forecasting Accuracy
- Technical Directive Incorporation
- Repair Production vs. Delivery Schedule
- Screening Steps in the Document Control Unit (DCU) Aeronautical Material Screening Unit (AMSU) Production Control (PC).

(5) Plant Supply. Plant Supply functions provides direct support to the activity’s operations and maintenance processes. In general, Plant Supply is part of the integrated system that receives requirements for goods and services, then fills those needs through the management of inventories or procurement from various sources of supply. It is fully integrated with Wholesale Supply functions for material management, procurement, visibility and access. Plant supply functions include Requirements Determination, Material Requirements Planning, Inventory Management, Warehouse Management, Procurement, and Environmental Health and Safety for monitoring and management of the following:

- Timely delivery of goods or service to the ultimate consumer
- Accurate status and information to the customer on the delivery of goods or service

- Total material visibility and access of material held by the activity and the enterprise
- Efficient and timely credit card purchases, including Bank Card reconciliation
- Inventory accuracy and reduction of overall inventory levels, including improved material availability and reduced customer wait-time
- Procurement, tracking and usage of only allowed hazardous materials by the activity

(6) Wholesale Supply. Supply functions include Forecasting, Supply and Demand Planning, Inventory Management, Buy/Repair Planning, Order Fulfillment, Advanced Planning, Serial Number Tracking, Allowance Development, Provisioning and Cataloging, Outfitting, Weapon System Monitoring, and End-of-Service Life Planning. Comprehensive integration would include Plant Supply functions for material management, procurement, visibility and access. These functions are designed to assist the following monitoring and management functions:

- Inventory Control Point (ICP) Response Time moving to Average Customer Wait Time (ACWT)
- Budget Constrained Planning and ‘What-If’ Analysis
- Stock-out Rate
- Supply Material Availability (SMA)/Fill Rate
- In-Transit Losses/In-Transit Write-Offs

- Total material visibility and access of material held by the activity and the enterprise
- NIIN Inventory Visibility by Condition and Quantity, and
- Forecasting Accuracy

(7) Travel Management. Functions include data availability and accessibility to sustain a seamless, paperless temporary duty travel system meeting the needs of travelers, commanders and process owners, including reducing processing costs and supporting mission requirements. Travel Management functionality is meant to provide:

- Increased capability to track individual travel orders and vouchers, and
- Increased efficiency in routing, approval and notifications within the travel process.

(8) Work Force Management. Workforce Management functionality is meant to provide:

- Processing of time records against project WBS/maintenance work orders/cost objects for total Navy Enterprise workforce (Civilian, Military, and Contractor)
- Improved workforce availability against required project tasks
- Training support related to localized attainment of certifications, licenses, qualifications and achievements not covered by position skill requirements or community profiles

- An integrated view of force resources span-of-control for total Navy Enterprise workforce
- Data for tracking historical workforce allocations against WBS/maintenance work orders
- Interfaces to authoritative sources, e.g., one-way or pulled.

Finally, pre-filled data fields from authoritative sources are not to be modified by COTS software or users, and current and planned major manpower and personnel systems will not be replaced by, nor their functionality duplicated in Navy ERP.

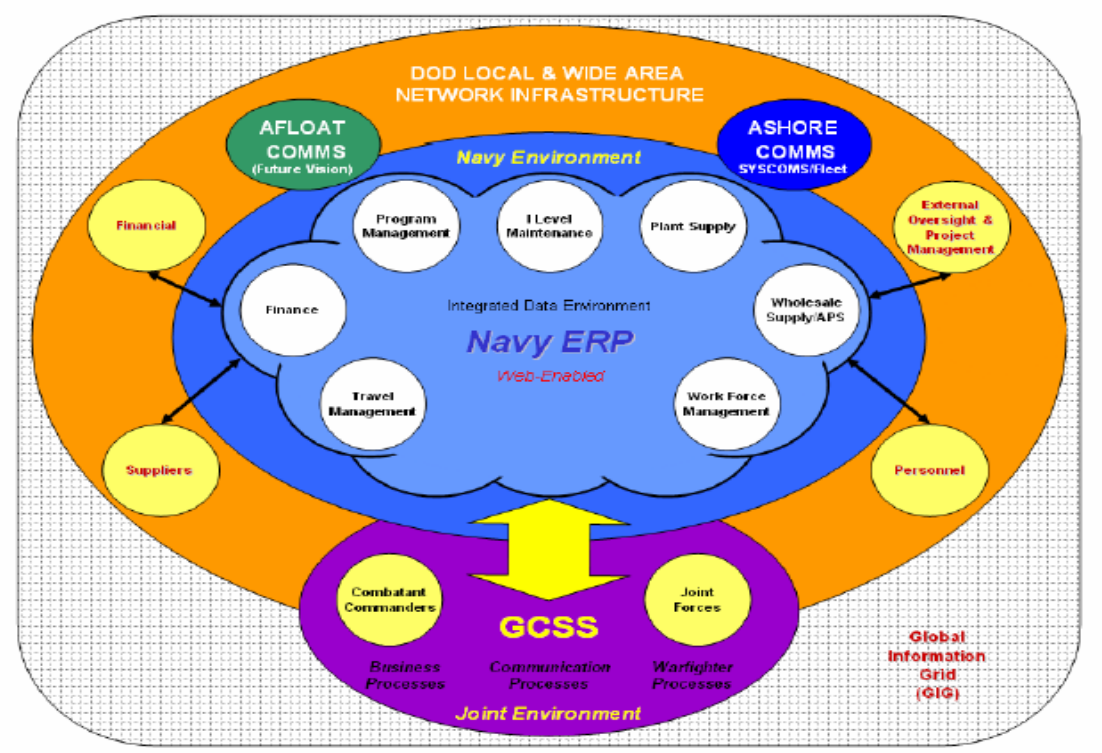

Figure 15. Navy ERP Program High Level Operation Concept Graphic (Navy ERP ORD, 2004)

f. Desired End State

The Navy ERP program desired end state updates and standardizes Navy business practices so that business activities are accomplished in the same manner anywhere in the Navy, using one set of commonly understood and accepted data, entered once, available securely anywhere in the Navy. This is designed to result in skill sets being more easily transportable, reducing retraining requirements, and improving overall job performance. Furthermore, the Navy ERP enables the Navy's Enterprise construct by providing a platform of integrated processes and information standards that unite previously disconnected functions in support of rapid and informed decision making. The implementation of Navy ERP looks to transform Navy's business processes while driving enterprise-wide efficiencies by providing managers with enterprise-wide financial transparency and total asset visibility. (Navy ERP, 2008)

2. Global Command and Control System – Maritime (GCCS-M)

a. Background

The Global Command and Control System - Maritime (GCCS-M) previously Joint Maritime Command Information System (JMCIS), is the Navy's primary fielded command and control System. The objective of the GCCS-M program is to enhance the operational commander's warfighting capability and aid in the decision-making process by receiving, retrieving, and displaying information relative to the current tactical situation. (GCCS-M, 1999)

b. Mission Need

GCCS-M is designed to provide improved functionality over the existing systems. The GCCS-M NTSP (1998) identifies the following new system features to overcome the shortcomings of existing systems:

- Integrated profiler capability, which provides the ability to quickly access various asset profiles
- Combat Direction System (CDS), the ability to perform real-time processing of tactical data from multiple interfaces (Ross, 1989)
- JAVA Image and Video Exploitation (JIVE)
- Joint Message Handling System (JMHS) PC features, including flat file UNIX/NT interface
- Faster and improved security features
- Improved track correlation, defined as selecting the most probable association between target tracks from a very large set of possibilities (Xiao & Xin & You, 2006).
- Extension of system to NT/PC environment allowing user to operate Tactical and non-Tactical standard applications
- Enhanced message processing capability
- Web-based interface to Naval Status of Forces (NSOF) data and Chief of Naval Operation’s Consolidated History File (CHF).

c. Concept of Operations

GCCS-M initiative is intended to be a near and mid-term implementation plan to meet fleet requirements to upgrade existing systems functionality. GCCS-M is not

intended to be a complete or final solution but will continue to evolve to meet requirements. The GCCS-M NTSP (1998) states the focus of GCCS-M is on six key tenets:

- Migrating from the JMCIS COE to the Defense Information Infrastructure (DII) COE. The introduction of the DII with its associated COE is the roadmap for achieving system interoperability across the Services.
- Migrating to PC Workstations and Servers. GCCS-M will begin a phased migration to the PC/Windows platform and away from UNIX-based workstations.
- Capitalizing on industry. GCCS-M Program Office is researching "best practices" within industry and evaluating unsolicited ideas from industry for use in increasing the efficiency of GCCS-M operations.
- Combining tactical and non-tactical networks. In cooperation with other programs, GCCS-M will merge tactical and non-tactical tasks onto a single workstation. Traditionally, these functions have been performed on separate machines that are connected to separate networks.
- Implementing cutting-edge logistics with a focus on training, maintenance, operational support, and configuration management. Improving service to the Fleet and reducing the present logistics train will include use of commercial logistics models, products and services.
- Streamlining the acquisition process. The three GCCS-M programs (Afloat, Ashore, and

Tactical/Mobile) are to be managed as a single program to the maximum extent possible.

d. Technical Capabilities Required

GCCS-M is the core command and control component of the Navy's Command, Control, Communications, Computers and Intelligence (C4I) systems. The system supplies information that aids Navy Commanders in a full range of tactical decisions. In functional terms, GCCS-M fuses, correlates, filters, and maintains raw data and displays image-building information as a tactical picture. Specifically, the system displays location of air, sea, and land units anywhere in the world and identifies whether those units represent friendly, neutral or enemy forces. It operates in near real-time and constantly updates unit positions and other situational awareness data. GCCS-M also records the data in appropriate databases, and maintains a history of the changes to those records. The user can then use the data individually or in concert with other data to construct relevant tactical pictures, using maps, charts, map overlays, topography, oceanographic, meteorological, imagery and all-source intelligence information all coordinated into what is known as a Common Operational Picture. The picture is referred to as common because once constructed it can be shared with other Joint, Coalition, and Allied users who need the information. This information allows commanders to review and evaluate the general tactical situation, determine and plan actions and operations, direct forces, synchronize tactical operations, and integrate force maneuver with firepower. The system operates in a variety of environments and supports command

and control of joint, coalition, and allied forces. Since 1989, GCCS-M has been fielded on Commercial Off-the-Shelf (COTS) hardware purchased from Sun Microsystems or Hewlett Packard. GCCS-M was one of the earliest widely fielded software intensive systems, and as such has been at the forefront of resolving COTS supportability, lifecycle, and maintenance issues. (Bullard, 2003)

e. System Description

GCCS-M receives, processes, displays, and manages data on the readiness of neutral, friendly, and hostile forces in order to execute the full range of Navy missions (e.g., strategic deterrence, sea control, power projection, etc.) in near-real-time via external communication channels, local area networks (LANs) and direct interfaces with other systems. The GCCS-M system is comprised of four main variants; Ashore, Afloat, Tactical/Mobile and Multi-Level Security (MLS) that together provide command and control information to warfighters in all naval environments. (GCCS-M NTSP, 1998)

The Ashore variant provides a single, integrated C4I capability to land-based forces in support of the warfighting requirements of commanders at all levels of the Navy and supported commands. The Ashore variant provides near real-time weapons targeting data to submarines; supports real-time tasking of Maritime Patrol Aircraft (MPA) assets; and supports the force scheduling requirements of the Navy. (GCCS-M NTSP, 1998)

The Afloat variant provides a single C4I capability to sea-based forces. It supports the Command, Control and Intelligence (C2I) mission requirements of the

Commander Joint Task Force (CJTF), Joint Navy Component Commander, Joint Force Air Component Commander (JFACC), Numbered Fleet Commanders, Officer-in-Tactical Command/Composite Warfare Commander (OTC/CWC), Commander Amphibious Task Force (CATF), Commander Landing Force (CLF), Ship's Commanding Officer/Tactical Action Officer (CO/TAO). The Afloat variant functions in a networked, client/server architecture featuring standard commercial hardware components and software applications. Afloat software components are comprised of core service modules, linked with mission applications through Application Program Interfaces (APIs) which is a technology that facilitates exchanging messages or data between two or more different software applications (Krechmer, 1992).

GCCS-M Tactical/Mobile Variant is comprised of both fixed sites and Mobile Variants. The fixed site is made up of Tactical Support Centers (TSCs), which is a fixed-site C4I system with satellite and point-to-point communications systems, Wide Area Network (WAN) capabilities, sensor analysis capabilities, avionics and weapons system interfaces, and facilities equipment. (GCCS-M NTSP, 1998) Tactical Mobile Variants (TMVs) are comprised of Mobile Operation Command and Control centers (MOCCs), which are rapidly-deployable, self-contained, C4I system that can be transported for contingency operations; Mobile Ashore Support Terminals (MASTs) which is a rapidly deployable basic C4I capability for remote locations, and Mobile Integrated Command Facilities (MICFACs), a deployable robust C4I system intended to support a commander and his staff ashore. (GCCS-M NTSP, 1998)

These sites provide the Navy Component Commander, the Maritime Sector Commander (Ashore), the Theater Commander (Ashore) or the Naval Liaison Element Commander (Ashore) with the capability to plan, direct, and control the tactical operations of Joint and Naval Expeditionary Forces (NEFs) and other assigned units within the respective area of responsibility. These operations include littoral and open ocean surveillance, anti-surface warfare, over-the-horizon targeting, counter-drug operations, power projection, antisubmarine warfare, mining, search and rescue, force protection, and special operations. (GCCS-M NTSP, 1998)

GCCS-M Multi-Level Security (MLS) Variant provides the structure to build, develop and install technology applications and systems to enable warfighters operating in a joint/coalition environment to access, retrieve, process, and disseminate all necessary information for maintenance of a consistent Common Operating Picture (COP), a single identical display of relevant information shared by more than one command facilitating collaborative planning and providing situational awareness (USJFCOM, 2008). MLS will provide a multi-level secure intelligence system providing on-line, automated, near real-time support to National, Joint and Naval Commanders; providing local and global networking for on-demand services and timely response to consumer requests for fused intelligence; and supporting joint Air Force, Army, Navy, Marine Corps, and Coast Guard counter terrorism, counter narcotics and allied coalition operations. (GCCS-M NTSP, 1998)

f. Desired End State

The desired end state is to provide Maritime Commanders at all echelons of command with a single, integrated, scalable Command, Control, Communications, Computers and Intelligence (C4I) system that fuses, correlates, filters, maintains and displays location and attribute information on friendly, hostile and neutral land, sea and air forces. It integrates this data with available intelligence and environmental information in support of command decision-making. (DoN RDA, 2008)

D. UNITED STATES MARINE CORPS PROGRAMS

This section summarizes two of the major acquisition programs for the USMC. These systems are the Marine Corps Enterprise Information Technology Services (MCEITS), a business initiative, and the Global Combat Support System – Marine Corps (GCSS-MC), a tactical system.

1. Marine Corps Enterprise Information Technology Services (MCEITS)

a. Background

The Marine Corps Chief Information Officer (CIO), from its inception, has been coordinating with representatives from the DoD, the DoN, and throughout the Marine Corps to establish an information technology infrastructure that better integrates work processes and information flows with technology to achieve the mission and strategic goals. To achieve this vision, the Marine Corps CIO began the Marine Corps Enterprise IT Services (MCEITS) initiative. MCEITS is designed to align the Marine Corps IT

resources (manpower, skill sets, hardware, software, facilities, programs, and budget) to create a shared IT services and information environment for all Marines, and establish an IT infrastructure that provides enhanced information access and information management. (Concepts and Programs, 2004)

b. Mission Need

The existing Marine Corps IT infrastructure was not originally designed and implemented as an integrated enterprise, nor was it employed to develop, provide or use capabilities made available by technologies designed to implement the concepts designed around Net-Centric Operations. (CDD MCEITS, 2007)

The following are gaps identified in the existing infrastructure:

- System Interoperability – Systems unable to fully support interoperability and security in a distributed environment; failure to use open standards and interfaces to permit cross-domain flow of information; integration and interoperability of existing and future systems.
- Information Access – Existing systems focused at the Service level; users are unaware that needed data already exists; information exchange in response to events or requests is not available; rapidly indexed/cataloged, distributed, stored, searchable, and retrievable information is not available; information is not uniformly tagged; web-based capabilities to access/search, generate, post, or

advertise mission-relevant information are not sufficient.

- Collaboration – Users cannot consistently and effectively interact in real time; lack of relevancy due to time lag; inefficient collaborative exchange of information within warfighting and business mission areas; inefficient performance of readiness reporting; joint total asset visibility.
- Cross-Domain Security – Users are unable to access data due to security, technical challenges, or organizational boundaries; information exchange problems with our authorized allied, coalition partners, and non-DoD users; lack of broad access to national imagery/intelligence databases and integration of theater produced intelligence.
- Information Exchange – Minimal capability to process multiple languages of both spoken language and applications; inability to capture cultural context in which humans function; heavy reliance on text message formats and inability to process multimedia presentations; lacking ability to associate information or data element security classification levels, releasability, and Special Handling Caveats; mediation of multiple spoken and computer-based languages; advanced information exchange, e.g., web-based messaging; minimal capability to process multiple languages limits the effective presentation of information.
- System Responsiveness – Increased demands for data storage capacity, transmission speeds, and information availability; unacceptably slow access

to pull or push data even when user has mission priority; intelligence and analysis are not forwarded to national database with sufficient robustness and timeliness. (CDD MCEITS, 2007)

c. Concept of Operations

The MCEITS program is meant to provide capabilities through an evolutionary, incremental acquisition block approach that will support globally interconnected command and control during all phases of warfighting. Additionally, each block will implement the designated MCEITS IT infrastructure and contain several spirals in order to implement the evolving DoD and industry technologies and standards for a net-centric Service Oriented Architecture (SOA), a collection of business services that communicate with each other (SOA, 2008), environment. Furthermore, MCEITS is designed to provide the infrastructure for a secure enterprise information environment to host and manage enterprise applications and services. (CDD MCEITS, 2007) The following capabilities support this overall concept:

- Information access through the dynamic discovery of services, content, metadata, and individuals improves information sharing, collaboration, and integrated situational awareness.
- Secure DoD approved collaboration to include text chat, chat rooms, presence information, instant messaging, shared applications, shared whiteboards, and the capacity to add audio and video to enhance the decision-making process. (CDD MCEITS, 2007)

d. Technical Capabilities Required

MCEITS is to implement a shared information environment where collaboration between providers and consumers of information takes place across loosely connected or coupled applications exposed as SOA. This evolving SOA capability, complete with technology, standards, and protocols is to drive the technology implemented by MCEITS. As an end-to-end capability, MCEITS should enable access to enterprise information and provide the ability to collaborate and share information across the business and warfighter domains. (CDD MCEITS, 2007)

MCEITS will accomplish this by implementing an IT infrastructure with application, service, and data environments. These capabilities are to provide responsive support for a secure, collaborative, interoperable data sharing environment while enabling the integration of products, services and users via a SOA.

The Marine Corps' net-centric interoperable capability is to be enabled via the Enterprise Application Environment (EAE) and Enterprise Services and Data Environment (ESDE) hosted within the MCEITS Platforms, Enterprise, Distributed, and Expeditionary. The EAE hosts and provides access to MCEITS provided applications as well as other enterprise-class systems and applications. The ESDE provides the environment for net-centric interoperability through the sharing of data and enterprise-wide discovery of people, content and services. Finally, a MCEITS Operations Center (MOC) is to be established to manage the MCEITS environment. (CDD MCEITS, 2007)

MCEITS Platforms serve as the processing infrastructure for other program elements to operate within.

The MCEITS Enterprise Platform consists of Enterprise IT Centers (EITC). The EITCs, as nodes of the MCEITS architecture, are the hosting environment to enable consolidation of enterprise applications, services, data storage and sharing. (CDD MCEITS, 2007)

The MCEITS Distributed Platform supports designated Marine Corps Installation (MCI) Commanders and their supported Marine Forces (MARFOR) Commander. The platform provides the environment to enable the MAGTF and Marine Corps Installations to use MCEITS services in garrison or when deployed. A Distributed node increases local accessibility and enterprise workload distribution by extending specific Enterprise platform services to designated base, posts or stations supported by MCI commanders. (CDD MCEITS, 2007)

The MCEITS Expeditionary Platform supports the deployed environment and is comprised of scaleable capability subsets that provide applications and services to the warfighter hosted at the Marine Expeditionary Force (MEF) and its Major Subordinate Commands (MSCs). The capability subsets are to enable interoperability for the MEF and MSC in theater as well as with the MEF Rear. (CDD MCEITS, 2007)

Within the platforms, the Enterprise Application Environment (EAE) is to provide the capability to operate and maintain hosted, managed or provisioned legacy systems and future Marine Corps applications that will benefit from incremental improvements using modular, reusable, and extensible software. The EAE hosts MCEITS-provided and other hosted enterprise-class applications, as well as provides the Enterprise Portal Framework (EPF) to enable a

personalized, user-defined, web-based presentation. The ESDE provides the environment within the platforms to exchange enterprise services, enable applications and programs to share capabilities, and provide access to authoritative data and other data repositories. (CDD MCEITS, 2007)

e. System Description

MCEITS will provide the infrastructure and a collection of capabilities to improve the ability to subscribe to existing information sources and collaborate with other users. This IT infrastructure and use of an adaptive overarching framework is to guide the Marine Corps transformation from existing legacy IT capabilities to an enterprise environment providing net-centric capabilities. This framework will consist of policies, principles, procedures, and tools to monitor and measure compliance as well as provide standard and interoperable architecture products, interoperable and reusable communication methods and data formats, core software products, and platforms to host and maintain enterprise applications, services and data environments. The infrastructure includes MCEITS Platforms (Enterprise, Distributed, and Expeditionary) with the hardware, software, and facilities infrastructure to implement the MCEITS hosted, managed or provisioned applications and services necessary to enable the collaboration and access to trusted information.

Implementation of MCEITS is to provide access for Marine Corps users to enable warfighting and business processes to the deployed Marine Expeditionary Force (MEF) level on both the NIPRNET and SIPRNET. (CDD MCEITS, 2007)

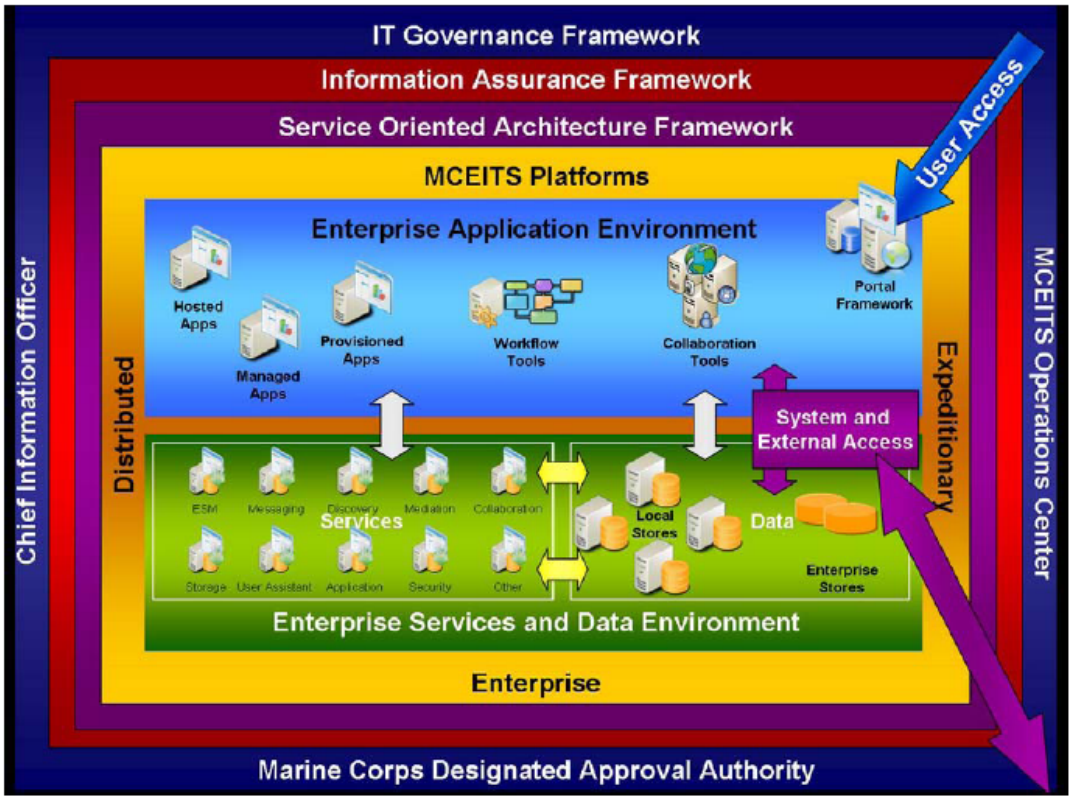

Figure 16. The MCEITS Framework (CDD MCEITS, 2007)

f. Desired End State

The Marine Corps will establish a net-centric supporting IT infrastructure enabled by a set of mutually supporting Enterprise IT Centers. These Enterprise IT Centers will be built, deployed, and maintained based on the interoperable architecture of the GIG and designed to support USMC migration to Net-Centric Operations. Marine Corps IT Centers will function as the focal point for the consolidation, realignment, and net enabling of the existing USMC environment of applications, databases, networks and facilities. These sites will be supported by a centrally-managed concentration of highly skilled technical staff

necessary for rapid design, integration, deployment, sustainment, and maintenance of net-centric enabled services and required supporting infrastructure. (CDD MCEITS, 2007)

2. Global Combat Support System – Marine Corps (GCSS-MC)

a. Background

The Deputy Commandant (DC), Installations and Logistics (I&L) is the Combat Service Support (CSS) advocate responsible for ensuring Marine Corps forces and, in particular, its deploying Marine Air Ground Task Forces (MAGTF's) contain the necessary CSS capabilities to meet mission requirements. The DC, I&L has identified those CSS capabilities as those capabilities, supplies, personnel and equipment necessary to support a MAGTF from the beginning of operations to the completion of its mission. (I&L, 2008)

b. Mission Need

The GCSS-MC ORD (2003) has identified the following shortcomings of existing Marine Corps logistics information systems:

- Current Marine Corps logistics information systems are primarily non-integrated and support organizations on a local level only.
- Current systems are characterized by non-standard human to computer interfaces, unnecessarily complex processes, non-standard data with high error rates and significant delays in information exchange. Furthermore, current systems force users to learn the intricacies of the computer system vice the specifics of the CSS process.

- The processes associated with current systems often deal with high volume, individual entries; paper-based forms; high transaction rates; and multiple levels of authorization, approval, or audit.
- Legacy systems were designed to support specific functional processes leading to non-interoperable “stovepiped” systems that are comprised of many interfaces that are expensive to develop and maintain.
- The enterprise’s lack of cross- functional decision support tools makes it difficult for commanders to analyze and act on CSS information. Current system software was built for specific hardware and cannot be easily and economically transferred to different hardware. Finally, they do not provide for the effectiveness gains that are possible with an enterprise view of logistics data and processes.
- The systems do not make use of labor saving technologies.
- Current systems do not provide real or near real time exchange of information.

c. Concept of Operations

GCSS-MC is the physical implementation of the enterprise information technology architecture designed to support combat support information requirements for both improved and enhanced MAGTF CSS functions and MAGTF Commander and Combatant Commanders. As such, GCSS-MC is not a single system but a portfolio of information technology capabilities tied to distinct performance measures that support required CSS mission objectives.

The GCSS-MC Portfolio will provide timely information to Marine Corps operational and CSS commanders, Combatant Commander's and Joint Task Force commanders and their staffs, and other authorized users. It will provide information interoperability and common logistics information applications and services across functional areas. GCSS-MC will allow operating forces commanders to base decisions on complete logistics information and make decisions in concert with specific operational tasks.
GCSS-MC will provide integrated functionality across supply, maintenance, transportation, finance, engineering, health, acquisition and manpower systems in accordance with the Marine Corps Logistics Operational Architecture. GCSS-MC supplies the users and operators of logistics processes access to information and applications regardless of location. (GCSS-MC ORD, 2003)

d. Technical Capabilities Required

Key technical components for the GCSS-MC portfolio, as detailed in the GCSS-MC ORD (2003), are the use of DoD standard Automatic Identification Technology (AIT) to support the accurate capturing of data, the shared data environment, a world wide web based capability to support access to applications and data, and the use of the Joint Technical Architecture (JTA), which is defined as the DoD standard for interoperability guidelines at system and component interfaces (Kerner, 2002).

- Uses of DoD standard AIT – Joint contracts have been established for the procurement of AIT devices with the intent of using these devices to automate manual functions wherever practicable. The GCSS-MC

portfolio will include in it software applications that utilize AIT devices for regular business processes such as receipting, inventorying, issuing, etc. in support of the functional processes of distribution, maintenance, and supply, at a minimum.

- Shared Data Environment – In order for GCSS-MC to meet the Combatant Commanders information requirements, any authorized user must publish the data managed and generated by the GCSS-MC portfolio to the Network-Centric Enterprise Services (NCES) environment for access. NCES will provide a common set of interoperable information capabilities in the GIG to access, collect, process, store, disseminate, and manage information on demand for war fighters, policy makers, and support organizations. The establishment of the Shared Data Environment is essential to the success of the program and remains a key technical component of the program.
- World Wide Web-based Capability – The USMC is expeditionary in nature and will always have MAGTFs forward deployed in support of the Nation’s missions. Accordingly, the applications in the GCSS-MC portfolio must be accessible via the World Wide Web in order to minimize the equipment footprint of deployed supported and supporting units.
- Use of JTA – In planning and creating the correct technical architecture to support deployed units, the GCSS-MC program must plan for and utilize the JTA to ensure compatibility of networks and that information will flow from GCSS-MC applications to

joint applications in an uninterrupted and timely manner.

- Components of the GCSS-MC portfolio will examine the application of artificial intelligence and expert systems to provide decision support and execution of CSS functions.
- GCSS-MC will maximize the use of military, government, and commercial communications and infrastructure services to support reliability and availability of GCSS-MC services. (GCSS-MC ORD, 2003)

e. System Description

GCSS-MC is an overarching capability environment (vice a discrete system) providing universal access to information and the interoperability of that information with logistics and other support functions. Compliance with GCSS-MC will ensure that information can be shared not only among multiple logistics functions, but also with joint and coalition partners. (I&L, 2008)

GCSS-MC is the Marine Corps portion of the overarching Global Combat Support System Family of Systems (GCSS FoS). GCSS-MC is the DC I&L's number one modernization priority and represents the "way ahead" for ground logistics information technology (IT). The goals of GCSS-MC are to support the operating forces as the primary customer, to provide a single point of entry for all supported units to request products and services, to provide access to a shared data environment, to satisfy the Combatant Commander/Joint Task Force (CC/JTF) information requirements, and to provide

the IT tools that will support the implementation of the Marine Corps Logistics Operational Architecture. (I&L, 2008)

GCSS-MC will be employed from the garrison environment to a deployed tactical environment with Marine Air Ground Task Forces. Its Internet protocol based architecture and infrastructure, will allow for the GCSS-MC services and applications to be accessible to any authorized user from any computer in any operational environment. From an internet (web) based interface, any supporting unit will be able to request and track the status of products (supplies, personnel, etc.) and services (maintenance, engineering, etc.). The supporting CSS unit will have the ability via GCSS-MC to process requirements, request and track the status of products and services from higher echelons and commercial vendors, and conduct tactical and operational CSS mission planning and execution functions. Using GCSS-MC, supporting establishment organizations will be able to sustain tactical CSS units as well as conduct strategic and enterprise level l logistic and acquisition functions in support of the Marine Corps mission. (GCSS-MC ORD, 2003)

f. Desired End State

The required end-state is represented by a portfolio of robust capabilities reflecting industry standards, supporting peace and employed wartime logistics requirements and satisfying MAGTF requirements for expeditionary logistics support. The end-state plans to ensure the availability of superior techniques, tactics, procedures, business rules, organizational models and

information technology with the hope of improving logistics support to the warfighter. (LOGMOD, 2005)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COMPARATIVE ALIGNMENT ANALYSES OF SELECTED DEFENSE ACQUISITION AND INFORMATION TECHNOLOGY STRATEGIES

A. INTRODUCTION

This chapter compares defense business strategies with Information Technology (IT) strategies in terms of the extent to which they appear to be in relative alignment. Specifically, defense acquisitions detailed in Chapter III are analyzed in terms of apparent fit among IT strategies and themes identified in Chapter II. A macro assessment shows various substantial parallels and some gaps in terms of the extent to which the various acquisition strategies are interrelated or mutually supporting.

B. ALIGNMENT

1. Alignment Construct as Assessment Criterion

The term alignment denotes an inter-relationship between or among relevant components. This notion is epitomized in *systems* theory, i.e., the fit, congruence or alignment of external (environmental) and internal organizational components affect and determine overall performance (Senge, 2006). Broadbent and Weill (1993) refer to alignment of business and IT strategy as “the extent to which business strategies were enabled, supported and stimulated by information strategies”. King and Teo (1996) define alignment as the “coordination between the business and IS planning functions and activities”. Luftman, Papp and Brier (1999) argue that “alignment focuses on activities

which management performs to achieve cohesive goals across the organization". A generalizable theme or premise is that the extent to which business and IT strategies are aligned affects and may be predictive of the overall systems performance, e.g., achievement of mutually reinforcing goals among inter-related strategies. This construct summarizes the theoretical perspective adopted in this research, i.e., alignment includes cohesive and concurrent intentions among relevant business and IT strategies. IT themes were identified in Chapter II and selected acquisitions were discussed in Chapter III. Gartlan and Shanks (2007) pertains.

2. Alignment as the Central Concept

According to Gartlan and Shanks (2007) alignment of business strategy and IT strategy is an important organizational issue that has plagued organizations for years. One underlying factor is the trend of businesses shifting from technology as a support function, to technology as an integral part of business strategy and operations. Luftman (2003) projects the strong vision of IT providing the driving force behind business transformation in the information age.

3. Alignment is a Relative Concept

This section discusses the relative alignment of selected acquisition programs (Chapter III refers) with existing defense IT strategies (Chapter II refers). Alignment of acquisition programs with IT strategies was based on whether or not the program met the defined description of the IT themes identified. For instance, if

program documentation discussed Net-Centricity as being an objective of the program, that program was then considered to be in alignment with the IT theme of Net-Centricity.

a. Structure of discussed alignment

The following subsections are laid out by IT themes. Within these subsections, the alignment of selected acquisition programs with that subsection theme is discussed.

b. Continuous Transformation Theme

The terms *continuous transformation* actually includes two different types of change – evolutionary, developmental or continuous change; and revolutionary or transformational change (Ackerman, 1986). The former stems from the U.S. quality movement in the 1980s whereby organizations use statistical process controls and other tools to continually improve all ongoing aspects of their business. There was of course a preceding quality revolution in 1950s Japan known as *Kaizen*. Transformational or gamma change is “like the caterpillar turning into the butterfly, is the emergence of a totally new state of being out of the remains of the old state” (Ackerman, 1986, p.48). As technological advancements increase at trigonometric rates in the industrial world, U.S. defense organizations are likewise attempting to revolutionize how technology and information systems can transform aging and legacy business processes.

Technology improvements and innovations are known to be crucial in the evolution of warfare. They can emerge incrementally at the margins - faster planes and heavier tanks - and they can be transformational and devastating, e.g., Ironclads in the U.S. Civil War, and two-way radios and German Blitzkrieg in WWII (Boot, 2007).

DoD is attempting to transform its personnel and pay systems using the Defense Information Management Human Resource System (DIMHRS). This system takes historically "stovepiped" Service requirements and integrates personnel and pay data into a single system. (DIMHRS ORD, 2005)

Additionally, DoD is shifting from a command and control structure comprised of joint and Service variations, into a single joint command and control architecture - the Joint Command and Control (JC2). The focus is shifting fundamentally from legacy and Service specific functions to Joint capabilities and execution. (JC2 ORD, 2002)

The existing collection of Navy "stovepiped" resource management systems imposes limitations on operational and support commanders in terms of being able to rapidly respond to emerging operational requirements, including limited ability to redirect assets as needed. Many of the systems and processes currently in use were designed to support functional organizations developed in the 1960s. (Navy ERP ORD, 2004) In response, the Navy is implementing an Enterprise Resource Planning (ERP) program providing a standardized set of tools developed using concepts from *business process reengineering* (Champy & Hammer, 1993).

The Marine Corps' current logistics information systems are primarily non-integrated and support organizations on a local level only. Additionally, the

business processes associated with current systems often deal with multiple levels of authorization, approval, or audit. With the goal of a renewed focus on supporting operating forces as the primary stakeholder, the Marine Corps is undertaking a new, more transformative approach through implementation of the Global Combat Support System-Marine Corps (GCSS-MC). This system provides a single point of entry for all supported units to request products, services and access to a shared data environment. (GCSS-MC ORD, 2003)

c. Net-Centric Theme

One working definition of net-centric includes the successful linking of compatible information systems with usable data to obtain needed information when and where needed (CIO, 2007).

Through web-based applications, DIMHRS will be accessible to all four Services allowing users access to a number of self-service functions. DIMHRS Home Page is the gateway to the following self-service functions: Personal Information, Benefits, Learning Management (Air Force only), Time Reporting, Payroll and Compensation, and Careers (DIMHRS, 2008).

Similarly, JC2 will be web-enabled and accessible to all relevant users. It will utilize Net-Centric Enterprise Services (NCES) for security including an adaptable command and control architecture. As vertical and horizontal interoperability continues to develop into a potent, force-enabling reality, the decision making process must be enhanced. (JC2 ORD, 2002)

Likewise, the pervasiveness of web-based services is integral in the development and implementation of the Navy ERP Program. In sum, users will be able to share, extract and exchange information with Joint systems by utilizing the Web-Enabled Navy (WEN) architecture and its Navy Enterprise Portal (NEP). (Navy ERP ORD, 2004)

Through the linking of external communication channels, local area networks (LANs), and direct interfaces with other systems, GCCS-M receives, processes, displays, and manages data on the readiness of neutral, friendly, and hostile forces. (GCCS-M NTSP, 1998)

Marine Corps Enterprise Information Technology Services (MCEITS) will establish a net-centric supporting IT infrastructure enabled by an optimal set of mutually supporting Enterprise IT Centers. It will function as the focal point for the consolidation, realignment, and net enabling of the existing USMC environment of applications, databases, networks and facilities. These Enterprise IT Centers will be built, deployed, and maintained based on the interoperable architecture of the Global Information Grid (GIG), designed to support USMC migration to Net-Centric Operations. (CDD MCEITS, 2007)

The Internet Protocol based architecture and infrastructure of GCSS-MC is designed to be accessible to any authorized user from any computer in any operational environment. From a web interface, any supported unit will be able to request and track the status of products, personnel and services, e.g., maintenance and engineering. (GCSS-MC ORD, 2003)

d. Information Operations Theme

Information Operations (IO) may not readily be perceived as a traditional warfighting function. The improving technology of integrating widespread and complex information systems now lies at the core of transacting a range of warfighting functions e.g., command and control, fires, maneuver, logistics, intelligence, and force protection. As knowledge is power, operational commanders pull-in, process and prioritize large quantities of data for the primary purpose of maintaining a superior view of the Common Operational Picture (COP) or conflict theatre, including external environmental factors and internal organizational capabilities. (Concepts and Programs, 2005)

DIMHRS facilitates administrative and warfighting functions by collecting, storing, transmitting, processing, and reporting personnel and pay data for all DoD personnel, including personnel locations and other relevant information. (DIMHRS ORD, 2005)

JC2 also supports administrative and warfighting functions by providing the capability to conduct deliberate and crisis action planning. Additional features include U.S. forces assessment, intelligence management and merged battlespace awareness. Current and projected disposition of hostile, neutral, and friendly forces can assist fluid decision-making. (JC2 ORD, 2002)

Navy ERP can depict operating force logistic needs and response requirements in administrative and contingency operations. (Navy ERP ORD, 2004)

The GCCS-M program receives, retrieves and displays information relative to dynamic or tactical situations. (GCCS-M NTSP, 1998)

MCEITS provides the warfighter with an infrastructure and a collection of capabilities that improves the ability to subscribe to existing information sources and collaborate with other warfighters which supports globally interconnected command and control during all phases of warfighting. (CDD MCEITS, 2007)

GCSS-MC provides universal access to information and the interoperability of that information with logistics and other support functions, e.g. a single point of entry for all supported units to request products and services. (GCSS-MC ORD, 2003)

e. Information Assurance (IA) Theme

Quite simply, the basis for the information assurance theme is to ensure that defense information and information systems have availability, integrity, authentication, confidentiality, and non-repudiation.

DIMHRS ORD (2005), JC2 ORD (2002), Navy ERP ORD (2004), CDD MCEITS (2007), and GCSS-MC ORD (2003) address the issue of IA through a certification and accreditation process that involves a series of policies and directives. These policies and directives assign responsibilities and prescribe procedures for certification and accreditation through a defense-in-depth approach that integrates personnel capabilities, operations and technology. This architecture contributes to the evolution to network centric warfare. As information assurance and interoperability

capabilities become integrated, Public Key Infrastructure (PKI) aspects will also pertain. The following policies and directives apply:

- DoDD 5000.1 - Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems.
- DoDI 5200.40 - DoD Information Technology Security Certification And Accreditation Process (DITSCAP)
- DoDD 8500.1 - Information Assurance (IA)
- DoDI 8500.2 - Information Assurance (IA) Implementation
- DoDI 8530.2. – Support to Computer Network Defense
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11 - National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products
- DoDI 8550.cc - Use of Mobile Code Technologies in DoD Information Systems
- The DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

f. Information Sharing Theme

Information sharing takes on additional complexity in the defense context. It includes making relevant information available to authorized participants, but can

also include cultural, managerial, and technical factors, and the ability to leverage off of shared data. (DoD Information Sharing Strategy, 2007)

DIMHRS employs standard business processes enabling the exchange of common information among the Service legacy personnel and pay systems and authorized external systems. (DIMHRS ORD, 2005)

JC2's Joint command and control architecture utilizes the GIG infrastructure to share access to data sources produced from Service, Agency, and theater-of-operations. JC2's shared data environment enhances information sharing, including access via web-enabled applications. The Joint Common Database (JCDB) is a fully integrated repository of information configured for and accessible by all users. It facilitates information sharing across Joint and multinational organizational boundaries. (JC2 ORD, 2002)

The Web-Enabled Navy (WEN) architecture, the target architecture of the Navy ERP, is meant to leverage industry best practices in terms of moving and sharing data. This provides accessibility and availability of information to authorized entities and to all applicable, authorized systems. (Navy ERP ORD, 2004)

Through the use of four main variants, GCCS-M shares command and control information with the warfighter. External communication channels, local area networks (LANs), and direct interfaces with other systems will enable warfighters operating in a joint/coalition environment to access, retrieve, process, and disseminate necessary information for maintenance of a consistent Common Operating

Picture (COP). The sharing of this information improves the commanders ability for command and control. (GCCS-M NTSP, 1998)

The MCEITS infrastructure supports the overall concept of information sharing by making a range of information accessible via DoD-approved collaboration tools, e.g., text chat, chat rooms, presence information, instant messaging, shared applications, shared whiteboards, audio and video. This infrastructure also enables cross-domain information sharing through the integration of several legacy C4ISR systems, and permits the integration of, or connection to, compatible C4ISR systems of allies and coalition partners. (CDD MCEITS, 2007)

GCSS-MC's environment provides access to information and the interoperability of that information with logistics and other support functions. Through the use of its internet protocol based architecture and infrastructure, GCSS-MC's services and applications can be shared among authorized users from any computer in the operational environment. These services and applications are to assist commanders' in the increasingly complex decision-making process. (GCSS-MC ORD, 2003)

g. Horizontal Integration Theme

Horizontal integration means the ability to integrate disparate information systems across functional units and/or across business lines. The point is to enhance speed of delivery and alignment across multiple entry contributions, i.e., commonality across a common set of business standards (ETP, 2007).

Through horizontal connectivity, DIMHRS meets the overarching goal of maintaining personnel information on individuals in Joint and multi-service units. This framework employs a fully integrated military personnel and pay capability for all Military Service components. (DIMHRS ORD, 2005)

JC2's goal of decision superiority is also reached through vertical and horizontal integration of joint command and control systems. Additionally, JC2's Mission Capability Packages (MCPs) support vertical/horizontal information exchange. This allows commanders and their staffs to analyze shared data, project requirements, analyze Blue, Red, Gray force location, and make time-sensitive decisions rather than relying on historical information from multiple, non-interoperable information systems. (JC2 ORD, 2002)

Horizontal integration is depicted in the Navy ERP Program's initial template (Template 1.0), addressing finance, program management, intermediate level maintenance, plant/wholesale supply, travel management and workforce management functions across the Naval maritime, aviation, nuclear, sustainment, and supply business areas. This provides Navy organizations with interoperable data elements for acquisition, financial, and logistics operations. (Navy ERP ORD, 2004)

GCSS-MC's integrated functionality across supply, maintenance, transportation, finance, engineering, acquisitions and manpower systems similarly provides information interoperability and common logistics information applications and services. The desired outcome

of these systems is to provide commanders' with across-function information integrated into a decision support array. (GCSS-MC ORD, 2003)

h. Governance Theme

Governance includes promoting standards and guidelines, ensuring a consistent well-defined direction, adjudicating disconnects, establishing legal and policy enforcement, and measuring performance (Information Sharing Strategy, 2007).

Figures 17 and 18 reflect traditional, top-down and hierarchical governance frameworks showing vertical levels of responsibility in DIMHRS and GCSS-MC respectively.

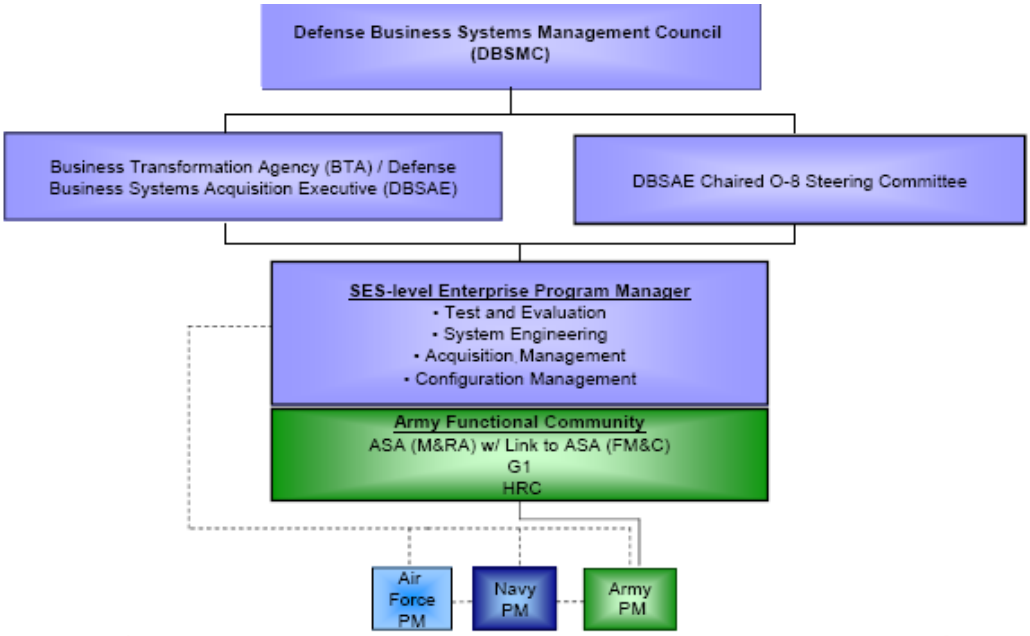

Figure 17. OSD-Level Governance (DIMHRS ADPO, 2008)

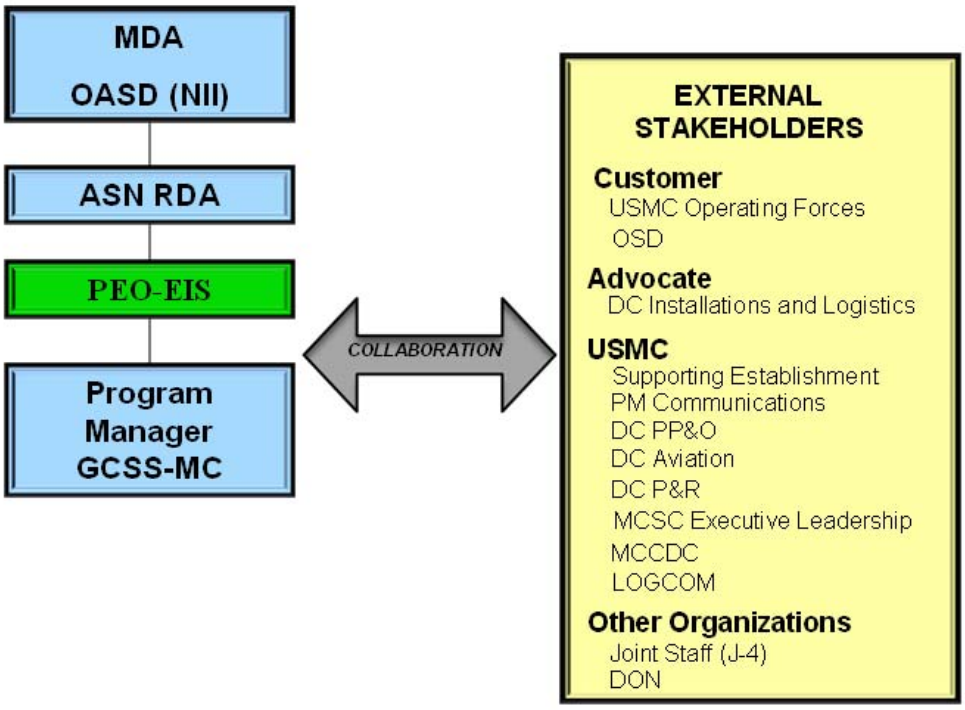

Figure 18. GCSS-MC/LCM Block 1 Governance (LOGMOD, 2008)

Navy ERP has a similar governance structure including five major functional areas: financial management, acquisition management, supply chain management, maintenance, and work force management as well as a process council overseeing end-to-end processes and assisting in resolving process and business rule issues. A board of advisors decides programmatic challenges. (SAP, 2008)

MCEITS will be governed by an IT Governance Framework consisting of policies, principles, procedures, and tools to monitor and measure compliance as well as provide standard and interoperable architecture products, interoperable and reusable communication methods and data

formats, core software products, and platforms to host and maintain enterprise applications, services and data environments (CDD MCEITS, 2007).

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. INTRODUCTION

This chapter draws conclusions on the degree of alignment between strategic documents and selected acquisition programs, e.g., (1) Department of Defense (DoD), Department of the Navy (DoN), and United States Marine Corps (USMC) information technology (IT) strategies; and (2) six defense acquisition programs. The former were explained in Chapter II, and the latter in Chapter III.

The concept of alignment considers cohesiveness and continuity between overarching strategic direction (documents) and actual IT programs. Also included is the notion of possible gaps between policy and strategic intent (themes) and six acquisition programs. Systems theory encapsulates crucial interrelationships among important components in terms of their relative alignment or congruence. This concept provides the theoretical foundation for drawing performance oriented conclusions in that, the fit of interrelated components working towards a common purpose determines overall performance (Senge, 2006).

Recommendations are also provided in this chapter to assist managers and practitioners in understanding and mitigating/managing gaps between defense IT themes and various acquisition programs. Recommendations for future study are also identified.

B. ALIGNMENT SUMMARIZATION

	Current Acquisition Programs					
Compiled IT Themes	DIMHRS	JC2	Navy ERP	GCCS-M	MCEITS	GCSS-MC
Continuous Transformation	X	X	X			X
Net-Centricity	X	X	X	X	X	X
Information Operations	X	X	X	X	X	X
Information Assurance	X	X	X		X	X
Information Sharing	X	X	X	X	X	X
Horizontal Integration	X	X	X			X
Governance	X		X		X	X

Table 2. Alignment Summarization

Table 2 illustrates nodes of apparent alignment and gaps between current acquisition programs and a compilation of IT themes gleaned from DoD, DoN, and USMC IT strategies (discussed in Chapter IV).

1. Continuous Transformation Theme

Continuous transformation here refers to the complex organizational – institutional in this case - capability to radically shift from lingering industrial era business processes into a globalized, web-enabled world. To the extent that defense planners internalize this fundamental change, one could expect that theme to be clearly embedded within acquisition program direction, documentation and practice. Unfortunately, analysis of GCCS-M and MCEITS planning documentation does not reflect this overarching concept.

In fairness, GCCS-M does provide functionality upgrades to the previous command and control system, Joint Maritime Command Information System (JMCIS). The *gap* is in terms of not appearing to provide sufficient direction and accommodation of existing and future technology. In sum, GCCS-M is an improved legacy system; designed to meet current needs/requirements without leaping into transformed territory.

MCEITS appears to take better advantage of emergent IT changes by ensuring information accessibility, but likewise, does not turn the transformative corner, i.e., current business processes are improved at the margins. In other words, the MCEITS infrastructure uses an adaptive overarching framework moving from existing legacy IT capabilities to an enterprise environment, but provides no improvement in the business processes (CDD MCEITS, 2007).

2. Information Assurance Theme

Information assurance involves availability, integrity, authenticity confidentiality, and non-repudiation of information and information systems.

The GCCS-M program receives, retrieves, and displays information which assists the decision-making process, but new IA concepts were not evident in supporting documentation and program development. For example, GCCS-M supports strategic deterrence, sea control, and power projection in near-real-time via external communication channels, local area networks (LANs) and direct interfaces with other systems, all of which require secure information (GCCS-M NTSP, 1998).

3. Horizontal Integration Theme

Horizontal integration is partly about removing electronic barriers among previously (stovepiped) business lines, thereby creating new cross-functional capability, i.e., integrated and redundant, end-to-end business standards.

The GCCS-M is a Service variant of the GCCS architecture. However, this Maritime command and control program variant does not appear to support joint commander decision making requirements. Collaborative information sharing and horizontal, joint command and control interoperability are not achieved. (JC2 ORD, 2002)

MCEITS does provide access to services and systems including information exchange and visibility, but similarly does not integrate end-to-end business standards across systems or processes.

4. Governance Theme

A governance theme includes promoting standards and guidelines, ensuring a consistent and well-defined direction, adjudication of disconnects, establishment of legal and policy enforcement, and measuring performance. As complexity might predict, IT governance and IT management are different concepts. IT governance leans towards decision rights, whereas IT management is about making and implementing specific IT decisions. IT governance is less about structure, establishing committees and boards, than it is about strategy and execution. (Failor, 2007)

Although JC2 and GCCS-M have an IT management structure, IT governance descriptions are absent or markedly blurred.

C. FINDINGS

1. Assumptions

Recommendations are based on the following assumptions:

- The selected strategic documents are directly applicable to the current and future direction of defense IT.
- Major IT themes were identified from the selected strategic documents.
- Acquisition program documents contained sufficient data needed to assess alignment.
- Programs will perform and function as documented.
- Program and strategic themes alignment includes the opposing notion of gaps.

2. Recommendations

Based on the stated assumptions, review of applicable literature and analysis of strategy-program alignment, the following six recommendations are offered. The purpose is to assist planners, IT managers and Service participants by providing a consolidated packaging of alignment and gap areas. The point is to support a unified effort in accomplishing the Defense, Navy and Marine Corps mandate to transform IT strategy.

a. A path from “As-is”, “To-be”

Relevant program documentation describes in detail mission needs, concept of operations, technical capabilities and systems descriptions; however, identifying how substantial details will be accomplished is unclear. For example, the JC2 ORD (2002) states: “Global Command and Control System (GCCS) will evolve from its current state of joint and Service variants to a single Joint C2 architecture and capabilities-based implementation comprised of mission capability packages and Global Information Grid (GIG) infrastructure, providing shared access to Service/Agency/theater-produced data sources”. Although the mission capability packages are clearly defined and the need for the Joint command and control architecture is generally understood, the method of connecting these capabilities to the GIG infrastructure, including providing shared access to all sources, is unclear.

Another example is contained within the DIMHRS ORD (2005): “DIMHRS (Personnel/Pay) shall operate within the framework of GCCS and the GCSS FoS...” “DIMHRS (Pers/Pay) shall exchange command and control (C2) information with GCCS and the GCSS FoS...”. The problem with these statements is two-fold: (1) JC2 was identified in the 2002 JC2 ORD as replacing GCCS; and (2) the semantics and interoperability level between DIMHRS and command and control information is not discussed. Without clarification on how these gaps are to be mitigated, it is reasonable to predict that programs will fall short of mission accomplishment.

b. Rapidly Changing Technology

A generally accepted business premise is that disparate legacy systems may be improved, but accommodating and leveraging available and emerging technological changes requires a “leap of faith” from an old, to a transformed new state (Ackerman, 1986). Indeed, some substantial aspect of the old system “dies” during true transformation. IT Program improvements are helpful, but must still be fundamentally reconceived to accomplish the transformation mandate.

c. IT Governance

All government IT acquisition programs have an IT management structure; however, a premise of this study is that for a program to be successful it must also have a tailored governance structure to drive and resource policies and implementation. An applicable governance structure should answer the following:

- What IT oriented and associated management decisions must be made? This question focuses on setting strategic direction, establishing enabling implementation structures, and following-through on evaluating desired outputs and outcomes.
- Who has decisional and input rights? The question implies accuracy and clarity in terms decision-making authority, responsibility and accountability for all important IT actions and behaviors.
- How are decisions formed and enacted? These are *process* issues encompassing organizational design, cultural norms, and control.

- Where begin the implementation of governance? The question is meant to imply that without effective governance, institutional focus becomes displaced or fragmented. (Failor, 2007)

A generally accepted problem in creating effective IT governance is obtaining the willing and thoughtful participation of senior military and civilian leaders not directly involved with IT. Additionally, IT community leaders must communicate requisite urgency up, down and across institutional arenas.

Joint development of IT principles is a crucial emerging stage differentiating legacy information management into a purple, defense IT architecture. In sum, consolidating joint IT principles is the foundation for effective IT governance, laying the groundwork for other governance mechanisms such as steering committees, councils and communities of interest (COIs). (Failor, 2007)

The figure below depicts a recommended approach to IT governance.

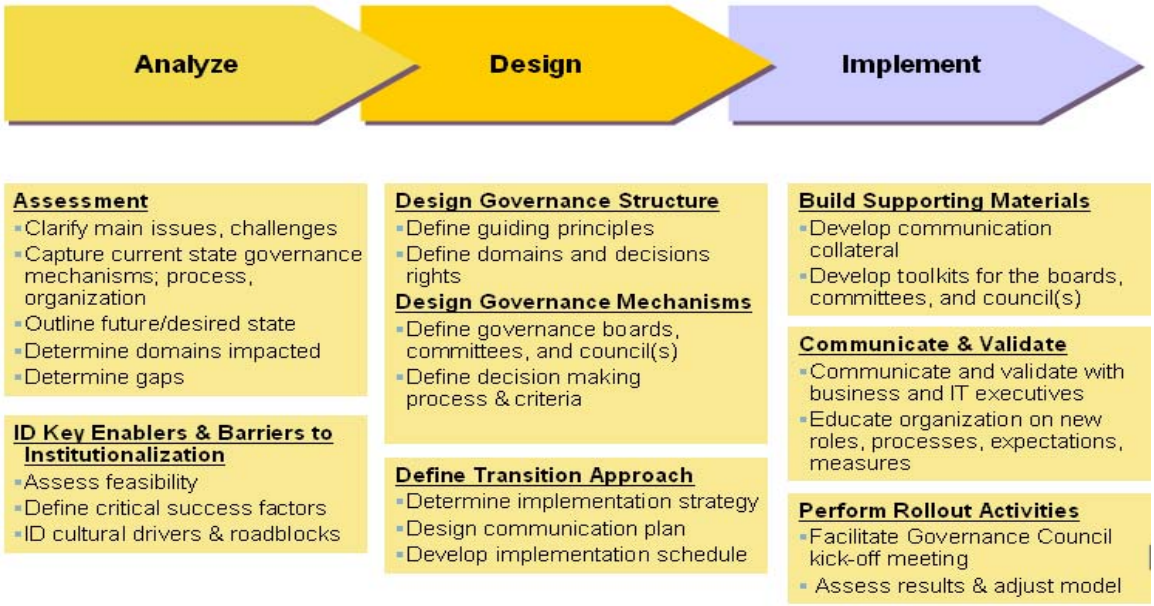

Figure 19. A Governance Approach (Failor, 2007)

d. Horizontal Atmosphere

Due to continued focus on joint warfare, IT horizontal program integration becomes vital. A joint commander unable to assess complex environmental and organizational information across Service lines is legacy, not transformation, and does not meet warfare requirements of the 21st century.

e. Security Measures

U.S. Defense is evolving into a net-centric architecture, and programs are becoming more accessible to warfighters. Unfortunately, this same capability provides adversaries with the potential for obtaining sensitive information. The cat and mouse game of building electronic

barriers and hacking through barriers - although not exciting by most accounts – must still be resourced and continually improved.

D. FUTURE WORK

1. Stakeholder Analysis

Since all acquisition programs are designed to meet identified stakeholder needs and requirements, then stakeholders are ideally suited to provide feedback on program plusses and shortcomings. Future studies could survey stakeholders, identify their needs, assess their power bases, and propose strategies to shift stakeholders into supportive categories.

2. Governance

Further research can be conducted distinguishing IT governance requirements from IT management issues to ensure both fields are sufficiently addressed.

3. DoD Acquisition Process

Further research can be conducted analyzing ongoing improvements and reforms in the DoD acquisition process. Addressed could be the extent to which defense practitioners develop and practice procurement practices reflected in private sector best practices, including how best to accommodate exponential changes in technology.

4. USMC Roadmap

Complete the ongoing design of a USMC IT roadmap that meets and is in accordance with DoD, DoN, and USMC strategies and policies.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ackerman, L. (1986). Development, transition or transformation: the question of change in organizations. *OD Practitioner.* December 1-8.

AFCEA international. (2008). Retrieved April 24, 2008, from http://www.afcea.org/factsheet.asp.

Alberts, D., Garstka, J., & Stein, F. (2000). Network centric warfare: Developing and leveraging information superiority. Washington, DC: National Defense University.

Application programming interface (API). (2007). Retrieved February 13, 2008, from http://www.sei.cmu.edu/str/descriptions/api.html.

Army's defense integrated human resources system (DIMHRS) program office (ADPO). (2008). Retrieved March 24, 2008, from https://www.hrc.army.mil/site/ArmyDIMHRS.

Base level information infrastructure (BLII): IT-21 enabler. (2008). Retrieved February 15, 2008, from http://www.chips.navy.mil/archives/98_jan/base_level.

Boot, M. (2007). War made new: Weapons, warfare, and the making of the modern world. New York, NY: Gotham Books.

Broadbent, M., & Weill, P. (1993). Improving business and information strategy alignment: Learning from the banking industry. *IBM Systems Journal*, 32(1), 162-179.

Bullard, Steven. (2003). A qualitative assessment and analysis of stakeholder expectations. Monterey, CA: Naval Postgraduate School.

Business transformation agency (BTA). (2007). Retrieved January 23, 2008, from http://www.defenselink.mil/bta/products/DBSAE_Portfolio/onepage/DIMHRS.pdf.

Center for Digital Government. (2005). Going beyond erp: A roadmap for transforming government enterprises. Folsom, CA.

Champy, J., & Hammer, M. (1993). Reengineering the corporation: a manifesto for business revolution. New York, NY: HarperBusiness.

CHIPS - the department of the navy information technology magazine. (2003). Retrieved February 14, 2008, from http://www.chips.navy.mil/archives/03_spring/webpagesTFW.htm.

Clinger, W., & Cohen, W. (1996). Information technology management reform act (Clinger-Cohen Act). Washington, DC.

Concepts and programs. (2007). Retrieved December 12, 2008, from http://hqinet001.hqmc.usmc.mil/p&r/concepts.htm.

Conway, J. (2006). Commandant's planning guidance. Washington, DC.

Cook, G., & Dyer, J. (2003). Business process reengineering with knowledge value added in support of the department of the navy chief information officer. Monterey, CA: Naval Postgraduate School.

Defense integrated military human resources system (DIMHRS). (2008). Retrieved March 10, 2008, from http://www.dimhrs.mil/.

Define meaning of loose coupling. (2008). Retrieved March 31, 2008, from http://looselycoupled.com/glossary/loose coupling.

Department of Defense Business Transformation Agency (BTA). (2006). Annual report to congressional defense committees, status of the department of defense's business transformation efforts. Washington, DC.

Department of Defense Business Transformation Agency. (2006). Enterprise transition plan (ETP) 2006 update. Washington, DC.

Department of Defense Business Transformation Agency. (2007). Enterprise transition plan (ETP) 2007. Washington, DC.

Department of the Navy, Headquarters United States Marine Corps. (2000). Marine corps strategy 21. Washington, DC.

Department of the Navy. (2002). Naval power 21. Washington, DC.

Department of the navy research, development & acquisition (DoN RDA). (2008). Retrieved February 22, 2008, from http://acquisition.navy.mil/programs/information_communications/gccs_m.

Department of the Navy. (2002). Sea power 21. Washington, DC.

DoD dictionary of military and associated terms. (2008). Retrieved March 31, 2008, from http://www.dtic.mil/doctrine/jel/doddict/.

Failor, M. (2007). Creating agile governance. Stamford, CT: Gartner, Inc.

Frequently asked questions (FAQ) for open systems. (2008). Retrieved April 2 2008, from http://www.sei.cmu.edu/.

GAO - dod's information assurance efforts. (2008). Retrieved April 24, 2008, from http://www.fas.org/irp/gao/nsiad-98132.htm.

Gartlan, J., & Shanks, G. (2007). The alignment of business and information technology strategy in Australia. *Australasian Journal of Information Systems*, 14(2).

Gartner Inc. (2006). Key questions that government IT strategic plans should address. Stamford, CT: Gartner, Inc.

Global command and control system - maritime (GCCS-M). (1999). Retrieved February 13, 2008, from http://www.fas.org/man/dod-101/sys/ship /weaps/gccs-m.htm.

Horizontal Integration. (2007). Retrieved November 19, 2007, from http://www.quickmba.com/strategy/horizontal-integration/.

Kerner, J. (2002). Joint technical architecture (JTA): Standards for interoperability. El Segundo, CA: The Aerospace Corporation.

King, W.R., & Teo, T. (1996). Integrating between business planning and information systems planning, *Information and Management*, 30, 309-321.

Krechmer, K. (1992). Interface APIs for wide area networks. *Business Communications Review*, 22, 72-4.

Krieg, K. (2007). Information Management for Net-Centric Operations. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics: Washington, DC.

Logistics modernization (LOGMOD) team east. (2008). Retrieved March 24, 2008, from http://www.lejeune.usmc.mil/lmt/.

Luftman, J.N., (2003). Competing in the information age: align in the sand. Oxford, New York, Oxford University Press.

Luftman, J.N., Papp, R. & Brier, T. (1999). Enablers and inhibitors of business-IT alignment. *Communications of the Association of Information Systems*, 1, 11.

Maconachy, W., Ragsdale, D., Schou, C., & Welch, D. (2001). A model for information assurance: An integrated approach. West Point, NY: United States Military Academy.

Marketing terms dictionary – American marketing association. (2007). Retrieved November 19, 2007, from http://www.marketingpower.com/mg-dictionary-view1406.php.

Merriam-Webster online. (2007). Retrieved November 19, 2007, from http://www.merriam-webster.com/.

Navy ERP - propelling transformation. (2008). Retrieved February 20, 2008, from http://www.erp.navy.mil/why.htm.

Office of the Under Secretary of Defense for Personnel and Readiness. (2004). Defense integrated military human resources system (DIMHRS) project overview. Washington, DC.

Ross, Debra. (1989). Object-Oriented database manager for the low cost combat direction system. Monterey, CA: Naval Postgraduate School.

SAP - transform your organization to meet today's public security threats. (2008). Retrieved March 24, 2008, from http://www.sap.com/industries/defense-security/index.epx.

Schwartz, K. (2007). ABC: An introduction to it governance. Retrieved December 6, 2007, from http://www.cio.com/article/111700#what.

Senge, P. M. (2006). Fifth discipline: The art and practice of the learning organization. New York, NY: Currency Doubleday.

Service-oriented architecture (SOA) definition. (2008). Retrieved February 21, 2008, from http://www.service-architecture.com/web-services/articles/service-oriented_architecture_soa_definition.html.

Strassmann, P. (1997). The squandered computer (1st ed.). New Canaan, Connecticut: The Information Economics Press.

Suttie, R. (2004). Navy Sea Power 21 Allies Project. Washington, DC: Naval War College.

Technical Services Organization (TSO). (2007). USMC integrated erp. Kansas City, MO.

United States Department of Defense, Chief Information Officer. (2007). DoD Information sharing strategy. Washington, DC.

United States Department of Defense, Chief Information Officer. (2003). DoD Net-Centric data strategy, Memorandum for Secretaries of the Military Departments. Washington, DC.

United States Department of Defense, Chief Information Officer. (2007). DoD Net-Centric services strategy. Washington, DC.

United States Department of Defense, Chief Information Officer. (2004). Data sharing in a net-centric department of defense. Washington, DC.

United States Department of Defense. (2004) Defense acquisition guidebook. Washington, DC.

United States Department of Defense, Chief Information Officer. (2006). Strategic plan. Washington, DC.

United States Department of Defense. (2005). Defense integrated military human resources system (Personnel and Pay) (ACAT IAM) operational requirements document 1.4. Washington, DC.

United States Department of Defense. (2005). Information technology portfolio management, DoD Directive 8115.01. Washington, DC.

United States Department of Defense, Joint Staff. (2002). Operational requirements document for joint command and control capability. Washington, DC.

United States Department of Defense. (2005). The national defense strategy of the united states of america. Washington, DC.

United States Department of Defense. (2003). Net-Centric data strategy. Washington, DC.

United States Department of Defense, Office of the Inspector General. (2002). Information technology acquisition and clinger-cohen act certification of the defense integrated military human resources system (DIHMRS). Arlington, VA.

United States Department of the Navy, N6. (1998). Global command and control system-maritime (GCCS-M) navy training system plan (NTSP). Washington, DC.

United States Department of the Navy, Office of the Chief of Naval Operations. (2004). Operational requirements document (ORD) for navy enterprise resource planning (ERP) program. Washington, DC.

United states joint forces command (USJFCOM): Glossary. (2008). Retrieved 2 February 2008, from http://www.jfcom.mil/about/glossary.htm#C.

United States Marine Corps. (2004). Concepts and programs 2004. Washington, DC.

United States Marine Corps. (2005) Concepts and programs 2005. Washington, DC.

United States Marine Corps, Headquarters Marine Corps. (2003). Operational requirements document for global combat support system-marine corps. Quantico, VA.

United states marine corps, installations and logistics (I&L). (2008). Retrieved February 11, 2008, from http://hqinet001.hqmc.usmc.mil/i&l/v2/LP/LPV/3/LPV3Mission.htm.

United states marine corps, logistics modernization (LOGMOD). (2008). Retrieved February 11, 2008, from http://www.lejeune.usmc.mil/lmt/FAQNEW.htm.

United States Marine Corps, Marine Corps Systems Command. (2007). Capability development document (CDD) for marine corps enterprise information technology services (MCEITS). Quantico, VA.

Wilson, C. (2007). Network-Centric operations: Background and oversight issues for congress. Washington, DC: Congressional Research Service.

Xin G., You H., & Xiao Y. (2006). Gray track-to-track correlation algorithm for distributed multitarget tracking system. *Signal Processing.* 86(11), 3448-3455 Retrieved February 22, 2008, from http://portal.acm.org/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Glenn Cook
   Naval Postgraduate School
   Monterey, California

8. Cary Simon
   Naval Postgraduate School
   Monterey, California

9. Richard Garcia
   Naval Postgraduate School
   Monterey, California

10. Joshua Sloan
    Naval Postgraduate School
    Monterey, California