United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

OUTSOURCING INFORMATION TECHNOLOGY SERVICES WITHIN THE DEPARTMENT OF DEFENSE: AN ANALYSIS OF THE NAVY/MARINE CORPS INTRANET PROJECT

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major G. J. Ormerod

AY 00-01

Mentor: Dr. C. D. McKenna
Approved: _____
Date: _____

Mentor: LtCol D. E. Houck
Approved: _____

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
23 Mar 2001	N/A	-

Title and Subtitle Outsourced Information Technology Services Within the Department of Defense: An Analysis of the Navy/Marine Corps Intranet Project	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Joint Military Operations Department Navy War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
The original document contains color images.

Abstract
The Navy/Marine Corps Intranet (NMCI) Project, as the largest service contract ever awarded ($7 Billion), represents a "Quantum Leap" in DOD Information Technology (IT) service requirements outsourced to a private contractor. The goal of the NMCI Project, as defined by the Navy, is to provide secure, seamless, global end-to-end communications connectivity, supporting both the warfighting and business functions. Due to the fact that this outsourcing venture is the first of its kind in sheer size and scope, several concerns have surfaced in regard to the implementation of the NMCI, especially from the Marine Corps' perspective. Based on the evidence available, it appears that outsourcing has been very successful in both commercial and governmental ventures to date. While the concept of it services outsourcing and sea management are relatively new, the efvidence suggests that the probable benefits that could be realized outweigh the potential risks involved. It is essential to understand that the NMCI is not a panacea - it will not solve all of Navy Department's it issues. However, in the long run, the Navy and Marine Corps' ability to interoperate and interface with other Joint Systems will be well worth the difficulties experienced in the short run.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 70	

REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

1. AGENCY USE ONLY (*LEAVE BLANK)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	23 MAR 2001	**STUDENT RESEARCH PAPER**

4. TITLE AND SUBTITLE
OUTSOURCED INFORMATION TECHNOLOGY SERVICES WITHIN THE DEPARTMENT OF DEFENSE: AN ANALYSIS OF THE NAVY/MARINE CORPS INTRANET PROJECT

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
MAJOR GERALD J. ORMEROD

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC COMMAND AND STAFF COLLEGE
2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
NONE

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
SAME AS #7.

10. SPONSORING/MONITORING AGENCY REPORT NUMBER:
NONE

11. SUPPLEMENTARY NOTES
NONE

12A. DISTRIBUTION/AVAILABILITY STATEMENT
NO RESTRICTIONS

12B. DISTRIBUTION CODE
N/A

13. ABSTRACT *(MAXIMUM 200 WORDS)*

THE NAVY/MARINE CORPS INTRANET (NMCI) PROJECT, AS THE LARGEST SERVICE CONTRACT EVER AWARDED ($7 BILLION), REPRESENTS A "QUANTUM LEAP" IN DOD INFORMATION TECHNOLOGY (IT) SERVICE REQUIREMENTS OUTSOURCED TO A PRIVATE CONTRACTOR. THE GOAL OF THE NMCI PROJECT, AS DEFINED BY THE NAVY, IS TO PROVIDE SECURE, SEAMLESS, GLOBAL END-TO-END COMMUNICATIONS CONNECTIVITY, SUPPORTING BOTH THE WARFIGHTING AND BUSINESS FUNCTIONS. DUE TO THE FACT THAT THIS OUTSOURCING VENTURE IS THE FIRST OF ITS KIND IN SHEER SIZE AND SCOPE, SEVERAL CONCERNS HAVE SURFACED IN REGARD TO THE IMPLEMENTATION OF THE NMCI, ESPECIALLY FROM THE MARINE CORPS' PERSPECTIVE. BASED ON THE EVIDENCE AVAILABLE, IT APPEARS THAT OUTSOURCING HAS BEEN VERY SUCCESSFULIN BOTH COMMERICAL AND GOVERNMENTAL VENTURES TO DATE. WHILE THE CONCEPT OF IT SERVICES OUTSOURCING AND SEAT MANAGEMENT ARE RELATIVELY NEW, THE EVIDENCE SUGGESTS THAT THE PROBABLE BENEFITS THAT COULD BE REALIZED OUTWEIGH THE POTENTIAL RISKS INVOLVED. IT IS ESSENTIAL TO UNDERSTAND THAT THE NMCI IS NOT A PANACEA – IT WILL NOT SOLVE ALL OF NAVY DEPARTMENT'S IT ISSUES. HOWEVER, IN THE LONG RUN, THE NAVY AND MARINE CORPS' ABILITY TO INTEROPERATE AND INTERFACE WITH OTHER JOINT SYSTEMS WILL BE WELL WORTH THE DIFFICULTIES EXPERIENCED IN THE SHORT RUN.

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH)
N/MCI, NMCI, NAVY/MARINE CORPS INTRANET, OUTSOURCING, IT, INFORMATION TECHNOLOGY SERVICES

15. NUMBER OF PAGES: **67**

16. PRICE CODE: **N/A**

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE:	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	**UNCLASSIFIED**	**UNCLASSIFIED**	

Date: _____

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

EXECUTIVE SUMMARY

Title: OUTSOURCING INFORMATION TECHNOLOGY SERVICES WITHIN THE DEPARTMENT OF DEFENSE: AN ANALYSIS OF THE NAVY/MARINE CORPS INTRANET (NMCI) PROJECT

Author: Major Gerald J. Ormerod 023 60 9854/3002 USMCR

Research Questions: Is the outsourcing of the Navy and Marine Corps' collective shore-based communications infrastructure to a private contractor a viable solution to the challenges that currently exist within the Department of Defense (DoD)? What are the benefits, risks, and critical concerns associated with the implementation of the NMCI?

Discussion:

The Navy/Marine Corps Intranet (NMCI) project is the single largest service contract ever awarded ($7 billion) in the history of the United States government. The NMCI project purports to represent a "quantum leap" in DoD Information Technology (IT) service requirements outsourced to a private contractor. The goal of the NMCI project, as defined by the Navy, is to provide secure, seamless, global end-to-end communications connectivity, supporting both the warfighting and business functions. It will also allow our military personnel to focus on the mission, rather than IT services, and will enable new processes and technologies to be integrated much faster and efficiently than before.

Due to the fact that this outsourcing venture is the first of its kind in sheer size and scope, several concerns have surfaced in regard to the implementation of the NMCI from the Marine Corps' perspective. To better examine these concerns, this paper looks at the current IT posture within DoD, the IT challenges within that posture, the history of outsourcing within DoD, and several key concepts involving IT management. The paper describes the NMCI project in detail and offers evidence to address the benefits, risks, and critical concerns of the implementation.

Conclusions:

Based on the evidence available, it appears that outsourcing has been very successful in both commercial and governmental ventures to date. While the concept of IT services outsourcing and seat management are relatively new, the evidence suggests that the probable benefits that could be realized outweigh the potential risks involved. The NMCI should not be considered as a panacea - it will not solve all of the Navy Department's IT issues. However, in the long run, the Navy and Marine Corps' ability to interoperate and interface with other joint systems will be well worth the difficulties experienced in the short run.

The critical concerns described in the paper are indeed significant, but are capable of being mitigated. It appears that both the DoN and the contractor have already established a solid foundation of coordination and cooperation in regards to resolving many of these concerns. As long as this "unity of effort" is focused towards the betterment of the NMCI structure, I predict tremendous success for this project and similar DoD ventures.

List of Illustrations

Page

List of Tables

Page

Table of Contents

Page

Chapter 1

Introduction

"Problems can not be solved at the same level of consciousness that created them"
- Albert Einstein

Purpose

The Navy/Marine Corps Intranet (NMCI) project is the single largest service contract ever awarded ($7 billion) in the history of the United States government. The NMCI project purports to represent a "quantum leap" in Department of Defense (DoD) Information Technology (IT) service requirements outsourced to a private contractor. The goal of the NMCI project, as defined by the Navy, is to provide the Department of the Navy secure, seamless, global end-to-end communications connectivity, supporting both warfighting and business functions. It will also allow our military personnel to focus on the mission, rather than IT services, and will enable new processes and technologies to be integrated much faster and efficiently than before.[1] Consequently, due to the fact that this outsourcing venture is the first of its kind in sheer size and scope, several concerns have surfaced in regard to the implementation of the NMCI from the Marine Corps' perspective.

Before we examine these concerns, we must take a closer look at the current Information Technology (IT) posture within the Defense Department, and an even closer look at several challenges within that posture which exist today. It will become apparent that the outsourcing of the Navy and Marine Corps' collective shore-based communications infrastructure to a private contractor is a viable solution to many of these challenges which plague DoD. To gain a better appreciation for the outsourcing concept, I will examine the concept in more detail and present

evidence of successful civilian and military IT outsourcing ventures to date. Outsourcing, while not a panacea, does offer numerous benefits that outweigh the risks involved. With that base of knowledge established, an analysis of these benefits and risks associated with the NMCI project can be conducted and the conventional concerns examined in detail. By the close of this paper, sufficient evidence should be offered to support the conclusions and answers to the research questions.

Research Questions

Primary Research Question:

- Is the outsourcing of the Navy and Marine Corps' collective shore-based communications infrastructure to a private contractor a viable solution to the challenges that currently plague the Navy Department?

Secondary Research Questions:

- From a Marine Corps' perspective, what are the benefits, risks, and critical concerns associated with the implementation of the Navy/Marine Corps Intranet project?
- Do the benefits outweigh the risks for the NMCI?
- Is the impact of the "critical concerns" identified manageable?

Chapter 2

The IT Challenge Within DoD

"There is no reason anyone would want a computer in their home"
- Ken Olson, President/Founder of Digital Equipment Corp., 1977

"I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won't last out the year"
– Editor, Prentice Hall, 1957

"Everything that can be invented has been invented"
- Charles H. Duell, Commissioner, U.S. Office of Patents, 1899

The information technology explosion of the last decade has spawned an unprecedented thirst for information and knowledge. The exponential growth of the Internet and subsequent exploitation of new global markets has forced industry to develop new, innovative systems and concepts to manage this boundless resource. The most significant concepts being studied and implemented in both corporate and governmental strategies today are *Information Superiority, Knowledge Management, Information Operations,* and *Information Assurance.*

The Department of Defense (DoD) is also struggling to take advantage of these emerging concepts and technologies in order to maintain its status as the premier military force in the world. Consequently, the Chairman of the Joint Chiefs of Staff (CJCS), in his Joint Vision 2020 (JV2020) publication, focuses on a need to transform America's armed forces so that they are "dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict."[2] The overarching focus of this vision is full spectrum dominance – achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. Rooted in these warfighting

concepts is the concept of *Information Superiority*. (see Figure 1). According to JV2020, "the continued development and proliferation of information technologies will substantially change

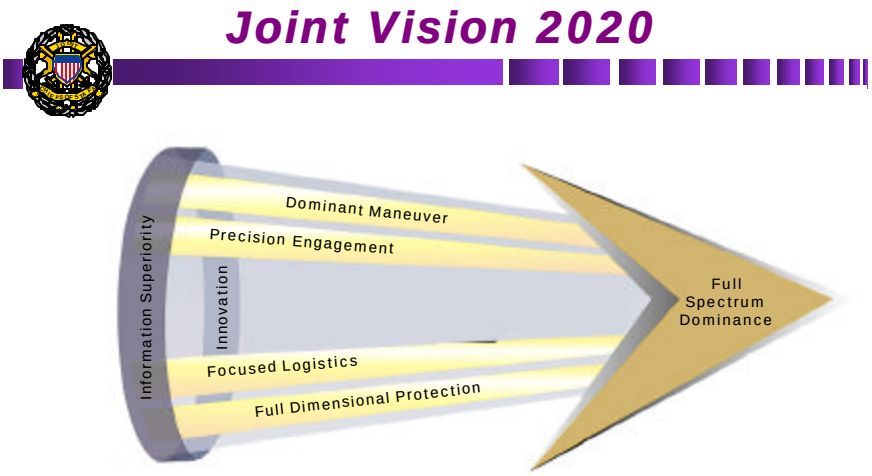

Figure 1: Joint Vision 2020[3]

the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control."[4] The realization that information superiority is integral to the goal of full spectrum dominance and the future of warfighting is the first step towards this transformation.

Information superiority itself is a somewhat abstract concept and can best be described as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[5] According to JV2020, this will provide a competitive advantage only when it is effectively translated into superior knowledge and decisions. The resultant "decision superiority" will allow for better decisions arrived at and implemented faster than an opponent's.[6]

Knowledge Management (KM), an embedded concept within Information Superiority, is a relatively new concept that evolved from Information Management. To better understand KM,

it is important to understand the differences between data, information, and knowledge. (refer to Figure 2). *Data* itself are discrete, objective facts about events - including numbers, letters, and images – without context. *Information* is data with some level of meaning, usually presented to describe a situation or condition. Therefore, information has an added value as compared to data. The definition of knowledge becomes more complex. *Knowledge* consists of truths, beliefs, perspectives, judgements, expectations, methodologies, and know-how. It is

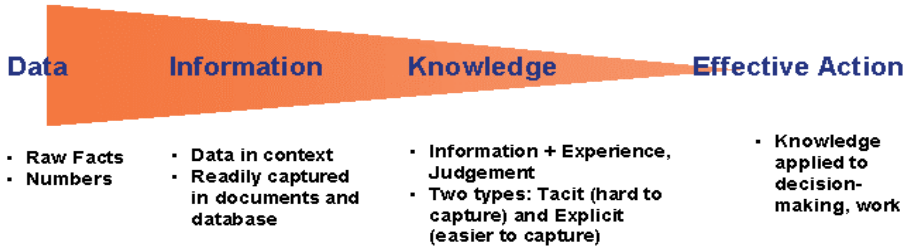

Figure 2: Data, Information, and Knowledge

accumulated, organized, integrated, and stored for indefinite periods of time to be applied to handle specific situations and problems. In summary then, knowledge is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information.[7]

Due mostly to the complexity of this concept, there are a multitude of differing opinions as to the actual definition of KM. The definition that is most common and relevant within the Department of Defense is simply "providing the right information to the right decision-maker at the right time."[8] KM's relationship to Information Superiority in a DoD context can best be summarized as follows:

> Knowledge Management offers the potential to significantly leverage the value of our IT investment and the intellectual capital of our people. Information technology and information management are essential, but alone, are insufficient to achieve information superiority. Knowledge management strategies facilitate collaborative information sharing to optimize strategic and tactical decisions, resulting in more effective and efficient mission performance.[9]

Two other concepts are inherently associated with information superiority, namely, *Information Assurance* and *Information Operations*. Information Assurance, as defined by Joint Pub 1-02, is "information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[10] Similarly, Information Operations (IOs) are "actions taken to affect adversary information and information systems while defending one's own information and information systems."[11] IOs can be either offensive or defensive in nature. Additionally, JV2020 also states that "information operations are essential to achieving full spectrum dominance. The joint force must be capable of conducting information operations, the purpose of which is to facilitate and protect US decision-making processes, and in a conflict, degrade those of an adversary."[12]

Knowing that KM and Information Superiority are important goals that DoD is striving to achieve, there are fundamental challenges that prevent their achievement. The ability to share information and knowledge on the scale envisioned by the CJCS is constrained by two predominant factors. First is the KM systems that are to manage the amount of data, information, and knowledge available; and second is the physical IT infrastructure interconnecting DoD. While KM concepts and systems are being fully explored and tested today, the IT infrastructure currently in place within DoD cannot support the <u>full</u> implementation of these new KM systems as envisioned in JV2020. Knowledge developed in one system is not necessarily available or compatible with other DoD systems. The current DoD IT network infrastructure consists of literally thousands of independent stovepiped systems and disparate informational networks that cannot be completely integrated. Due primarily to service

parochialism, funding constraints, and, ironically, the inability to share common system requirements over the past several decades, systems and networks were allowed to evolve independently with little compatibility requirement or configuration management. Consequently, this lack of standardization and incompatibility of systems negates any timely transition to a truly effective and efficient global network at this time. In defense of DoD, the policymakers and military leaders of the '70s and '80s had no idea of the quantum leap that information technology would make during the coming years.

As an analogy to help illustrate this problem, consider the evolution of the railway systems within the United States during the 1800s. While the use of rail dramatically improved the flow of materiel throughout the country, a significant problem arose concerning the standard gauge of the track (distance between rails). A rail system in Georgia was not necessarily the same as a rail system in Virginia. When these different systems would meet, cargo from one train had to be manually cross-loaded to a train on the other system. If we associate "information" with the cargo and "network protocols" with the differing rail systems, we can visualize the problem. As the cargo is converted from one rail system to the other, so must the information (data streams) be converted from one network or system to another. Subsequent standardization of rail gauges solved the problem. However, once a single standard gauge was established, all of the nonstandard rails had to be physically converted. This is a significant issue today with our IT network infrastructure within DoD. As standardizations and compatibility requirements are established, timely transitions must be effected across DoD.

Realizing this, DoD has placed considerable effort and resources into the development and implementation of numerous interoperable (joint) systems such as the Global Command & Control System (GCCS), the Joint Forces Requirements Generator II (JFRG II), and the Joint

Surveillance Target Attack Radar System (JSTARS), to name a few. As a secure environment in which these new systems could operate, a conceptual network infrastructure model known as the Global Information Grid (GIG) was developed. According to JV2020, the grid "will be the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel."[13] The development of these joint systems and the GIG is a monumental step towards the principles of KM and the accomplishment of the ultimate JV2020 goal of information superiority. However, as these new joint systems are being developed, DoD is having a difficult time effectively transitioning to a common IT network infrastructure, owing mostly to differing requirements and opinions among the services and agencies within DoD. In these times of budgetary constraints and calls for continued reductions in end strength, DoD simply does not possess the manpower, the money, or the necessary skill sets to accomplish this task on its own in an efficient and timely manner.

On the other hand, private industry is in a much better position to design, effect, and manage information networks while simultaneously integrating emerging information technologies. The civilian sector, being profit-based and not tied to governmental bureaucracy, has quickly and efficiently implemented the emerging IT concepts described earlier. The private IT industry, therefore, possesses the organization, experience, and flexibility required to implement the technical change that DoD so desperately needs.

The Department of the Navy (DoN), realizing these problems within its own network structure, recently made a bold decision to outsource the bulk of its shore-based IT network services infrastructure to the civilian sector for management. This monumental initiative, known as the Navy/Marine Corps Intranet (NMCI) project, features maximum reliance on commercial

business models and replaces government-owned/government-operated (GO/GO) infrastructure with a contractor responsible for providing a complete range of services. The NMCI concept, being such a significant deviation from the status quo of Navy management of Navy network infrastructure, has raised numerous issues for debate. However, before we address the details of the NMCI project, it is important to gain a better appreciation for outsourcing as a concept, and the history of outsourcing within the federal government, specifically within the US military. With a better historical perspective, an analysis of the inherent benefits and risks associated with the NMCI project can be conducted.

Chapter 3

The Evolution of IT Outsourcing

"Within the past decade, more than 85% of North American companies have outsourced at least one or more business functions"
- International Data Corporation, 1996

In its basic form, outsourcing is defined simply as acquiring a service rather than performing it yourself. The main purpose of outsourcing is to assign a task to another party who can perform it more efficiently and cost effectively than you. The popularity of the outsourcing concept continues to gain momentum in both the private and public sectors. Private corporations are turning to outsourcing for a wide range of functions from logistics to human resources to accounting. The federal government, through recent legislation, is also being forced to seriously examine its own internal functionality to determine which services can be outsourced.

The government, to include its armed forces, has long regarded outsourcing as a necessary function within its organization. Many traditional "blue collar" functions such as depot maintenance, base security, food service, and custodial work have been contracted out to the private sector for decades. However, in recent years a growing trend of traditionally "white collar" functions have begun to enter the realm of outsourcing, to include many business , logistics, and health care functions. Contractor augmentation has also become quite common in support of military operations throughout the world. For instance, over the last decade alone, the U.S. military has contracted out a multitude of logistics service requirements in support of numerous Military Operations Other Than War (MOOTW). This outsourced logistics support concept, known as LogCAP (Logistics Civilian Augmentation Program), was implemented by the U.S. Army in 1985 in response to severe organic logistical support shortfalls within its active duty force structure. Contracted LogCAP service providers such as Brown and Root have

provided essential services such as base camp construction, civil engineering, generator servicing, and power production in MOOTW environments such as Operation RESTORE HOPE in Somalia, UPHOLD DEMOCRACY in Haiti, SUPPORT HOPE in Rwanda, and JOINT ENDEAVOR in Bosnia. This outsourcing of military logistical requirements to contractors has proven extremely successful and should be viewed as a model for use in other functional arenas.[14]

The commercial IT world has followed a similar path of evolution. Initially, most IT tasks farmed out to contractors included menial functions that could be narrowly and easily defined, such as data entry and tape cleaning. However, with the growing capability of IT contractors to perform more complex tasks much more efficiently such as Wide Area Network (WAN) design, administration and system integration, a trend of IT outsourcing has logically followed suit.

This trend has accelerated recently as civilian corporations and governmental agencies have endeavored to become or remain more competitive. To do so, organizations are focusing on their "core competencies," or those functions that inherently define that particular organization. As an example, the core competencies of a car manufacturer should be designing, building, and selling cars – and not necessarily on the transportation of the new cars from the factory to the dealers. If this transportation requirement could be met more efficiently by an external trucking company, than outsourcing could be a viable solution. Like the successes realized in the logistics world, many IT outsourcing ventures in the private industry have proven successful, to include such business giants as GM, Xerox, and IBM. While a relatively new concept to the federal government, IT outsourcing does offer numerous advantages. The general

reasons for outsourcing IT services, according to federal managers, are as follows:[15]

- Budget realities
- Cost reduction
- Access to skilled personnel
- Improved IT responsiveness
- Help with legacy systems
- Improved business and customer service
- Implement new architecture

The federal government, realizing its own internal dysfunction in regards to its business practices, has taken enormous steps in the past decade to streamline itself. Consequently, much governmental legislation and policy has been introduced in order to effect this streamlining effort, especially in the realm of outsourcing service requirements to commercial activities.

Governmental Legislation and Policy

Since the mid-1950s, the United States' official policy has been to acquire needed goods and services from commercial sources. In 1955, President Eisenhower stated "the Federal government will not start or carry out any commercial activity to provide a service or product for its own use if such product or service can be procured from private enterprise through ordinary business channels."[16] Furthermore, OMB Circular A-76, *Performance of Commercial Activities*, first issued over 30 years ago, establishes Federal policy for the performance of "recurring commercial activities." The Circular was revised numerous times and supplemented in 1996. The 1996 supplement provides updated guidance and procedures for determining whether recurring commercial activities should be operated under contract with commercial sources or in-house using government facilities and personnel. A-76 further clarifies the policy by stating "the Government shall not start or carry on any activity to provide a commercial product or service if the product or service can be procured *more economically* from a commercial source"[17] (emphasis added).

Additionally, Circular A-76 Supplement, Appendix 5 (also titled Office of Federal Procurement Policy (OFPP) Letter 92-1) defines the distinction between those functions that are "inherently governmental" as compared to those that are "not inherently governmental." As may be obvious, not all government functions may be performed by contractors. As a matter of policy, an "inherently governmental function" is a function that is so intimately related to the public interest as to mandate performance by government employees. For example, the command of combat troops, the direct conduct of criminal investigations, the direction and control of intelligence and counter-intelligence operations, and the determination of budget policy, guidance, and strategy are all inherently governmental functions. Conversely, services that relate to budget preparation, support of acquisition planning, and prisoner detention are not inherently governmental examples.

Unfortunately, OFPP Letter 92-1 is rather vague in defining the specific functions of IT and whether they were deemed inherently governmental or not. Realizing the need for further clarification, the Department of the Navy published additional guidance that further delineates its IT functions:[18]

Inherently Governmental (in support of warfighting IT functions)	**Non-Inherently Governmental** (in support of shore-based garrison IT functions)
- Information Management	- IT Infrastructure Design and Development
- Knowledge Management	- IT Hardware/Software Deployment
- IM/IT Strategic Planning	- IT Maintenance
- IT Investment Management	- IT Infrastructure Operations
- IT Manpower Planning	- IT Customer Support Services
- IT Education and Training	- IT Education and Training
- IT Architecture	- Information Assurance
- IT Acquisition	
- IT Infrastructure Management	
- IT Infrastructure Operations	
- IT Customer Support Services	
- Information Operations	

Most of the IT functions that directly involve the operational or tactical warfighting systems and networks of military forces are designated as inherently governmental for obvious reasons. On the other hand, the shore-based garrison IT functions are distinctly non-inherently governmental. It is these shore-based functions that are a viable target for outsourcing within the DoN and constitute the bulk of the NMCI project

Congress and the Executive Branch also established significant initiatives recently to direct Federal agencies to conduct the government's affairs in a more business-like fashion. The three pieces of legislation that affect Federal outsourcing and the outsourcing methodology are the Clinger-Cohen Act (CCA) (formerly the Information Technology Management Reform Act (ITMRA)), the Government Performance Results Act (GPRA), and the Federal Acquisition Streamlining Act (FASA). Of the three, the CCA will be examined more closely since it has the most impact on IT outsourcing within the federal government.

With the passage of the Clinger-Cohen Act (CCA), Congress covered a wide range of functions, requiring agencies to perform the following:

- Develop an IT Architecture
- Determine who will perform the IT functions
- Develop performance-based work statements for contracting purposes
- Benchmark activities against those of the private sector
- Re-evaluate internal processes prior to making significant investments in IT
- Institute capital planning and investment control procedures

The CCA specifically requires that, prior to making an investment in a new information system, agencies must determine

> whether the function to be supported by the systems should be performed by the private sector, and if so, whether any component of the executive agency performing that function should be converted from a government organization to a private sector organization; or whether the function should be performed by the executive agency, and if so, whether the function should be performed by a private sector source under contract or by executive agency personnel.[19]

In summary, the government, through legislative and executive processes, has attempted to re-engineer itself by integrating the better business practices used in the commercial sector. Consequently, as outsourcing has become an important component within the government, it is now becoming essential to the efficient conduct of the military's business affairs as well. The IT functions described above as non-inherently governmental are now at the forefront of this outsourcing evolutionary path. The NMCI project then, although complex in and of itself, is simply the next logical step in this evolutionary process whereby the proven better business practices of the commercial IT industry have been applied against the IT infrastructure problems described in Chapter 2. While the concept of the NMCI project is logically sound, the implementation and transition may pose some unique challenges for the DoN. These challenges will be discussed in Chapters 6 and 7.

Having a better grasp now of the evolution of the outsourcing concept, its governing legislation and policy, and the inherently governmental/non-inherently governmental distinctions as they apply to the IT functional areas, we can now examine a new popular IT outsourcing mechanism known as *seat management*.

Chapter 4

The Seat Management Concept

Seat management, also known as desktop outsourcing, is a recent concept developed to allow organizations to focus on their respective core competencies by outsourcing the procurement and management of their desktop environment to an outside contractor. It is modeled after the telecommunications industry, with the idea that the computer is a utility much like a phone, and the service behind it should be transparent to the user. Since the fundamental tenets of the NMCI are derived from the seat management concept, we will spend some time exploring it in more detail.

Seat management is a performance-based, non-owned service that encompasses all aspects of the desktop environment and its associated network infrastructure. General seat management services available include:[20]

- Asset Management
- Technology Refresh
- User Support
- Engineering & Analytical Support
- Customer Services Support
- Deployment/Disposal of Equipment
- Infrastructure Management
- Transition/Migration of Services
- Operations & Maintenance Support
- Program Management Support

Seat management provides these capabilities in whole or in part as an information technology service that is paid for on a per-seat basis. Each seat can be "tailored" to fit the individual computing needs of that particular workstation. For example, a seat could range from a basic workstation with network access to a premium managerial workstation with Video Teleconferencing (VTC) capability, voice over data software, and SIPRNet (Secret IP-Routed Network) access. One could compare tailoring a seat within seat management to the purchase of a new automobile. Every sticker in the window always begins with a description of the options

included in the basic model. However, for every additional option desired there is an associated cost. A car "loaded" with extra options is often substantially more expensive than the basic model.

The General Services Administration (GSA), an early pioneer in the area of seat management within the federal government, recently established its Federal Computer Acquisition Center (FEDCAC) to serve as a broker to Federal agencies to provide seat management contract services. According to FEDCAC, the Seat Management contract,

> is a non-mandatory, multiple award, firm-fixed, ceiling-price, indefinite delivery, indefinite quantity (IDIQ) contract, with a base period of five years with one five year option. This contract will provide government agencies with desktop computing encompassing the management, operation, and maintenance of the desktop and its associated network infrastructure as a unified service. This service includes the entire suite of hardware, COTS software, connectivity, and support services required to support desktop computing in a business, engineering, scientific, or mixed work environment.[21]

FEDCAC now has standing contracts with several commercial IT service providers such as EER Systems, FDC Technologies, IBM Global Services, Multimax, PRC, Science Application International Corp., TechServ LLC, and Wang Government Services, Inc.[22]

Generally speaking, seat management is designed to help agencies keep abreast of the latest technology, obtain consolidated support services, reduce the need for in-house expertise, reduce the cost of IT ownership, establish a common operating environment, and match tools and software to mission requirements.[23]

The focus of seat management should be information technology infrastructure and services outsourcing. The real issue is whether an agency should outsource its IT infrastructure, not whether they should use seat management.[24] Through outsourcing, agencies can theoretically save on in-house developmental, service, and support costs. Through seat

management, an agency could obtain more efficient, effective, interoperable IT products and services that support the agency's mission.

However, deciding on the collection of services needed requires a great deal of planning on an organization's part before a seat management solution comes into the picture. "You've got some cultural issues to deal with right off the bat because you're turning over control of the day-to-day technical support functions and oversight of the hardware and software functions to one single vendor," said John Okay, senior vice president of Federal Sources Inc., a research firm in Vienna, VA. "That's a big change for most agencies."[25]

Examples of successful seat management implementations within the Federal government include the Outsourcing Desktop Initiative for NASA (ODIN) and the Bureau of Alcohol, Tobacco, and Firearms (ATF). Under ODIN, NASA's Jet Propulsion Laboratory outsourced the ownership and management of 8,000 or so desktop computers and associated network infrastructure to OAO Corporation in 1997. The five-year, $200 million contract enabled the organization to focus on its core mission. According to Richard Green, deputy manager of JPL Institutional Computing and Information Services, "we're in the outer space exploration business, not the PC management business."[26]

The Total Cost of Ownership

Prior to pursuing any type of IT venture, whether simple contractor augmentation for a particular project or a complete seat management outsourcing contract, the organization must understand the costs associated with its IT environment. These collective costs, known in the business community as Total Cost of Ownership (TCO), pose a significant challenge to any organization since they can be quite difficult to quantify. Once an organization knows exactly how and where it spends its money supporting its IT environment, it can then seek to compare

and contrast initiatives such as seat management in order to cut costs. An organization entering into a seat management contract without doing its TCO "homework," may be setting itself up for financial disaster. Referring back to the car manufacturing analogy in Chapter 3, the auto producer must know the actual TCO for its transportation requirement before it could possibly accept an outsourcing contract from an external trucking company. How else could the car company know if the service was provided more economically or not?

As mentioned earlier, understanding the TCO of an organization's IT environment can be quite difficult. A TCO model, or template, helps track how much money is being spent managing an existing IT environment including service, support, training, upgrades, procurement, policies, and management. TCO analysis consists of identifying direct costs and indirect costs associated within an IT environment.

Direct costs are the capital, fees, and labor costs spent by the organization's Information Systems (IS) department in delivering IT services and solutions to the organization and its users. Costs include hardware and software expenses, IS operations labor, service desk labor, and other actual costs related to clients, servers, peripherals, and network.[27]

Indirect costs are more difficult to determine. They measure the efficiency of IS in delivering expected services to the users. If the IS management and solutions are efficient, users are less likely to be burdened with self and peer support, as well as downtime. Conversely, if the IS management and solutions are inefficient, users typically must spend more time supporting themselves and each other, and are impacted by more downtime. These costs often are hidden in most organizations and are not measured or tracked.[28]

To meet this new demand for TCO modeling, several analyst firms have emerged that provide TCO models. Gartner Group, Forrester, Harris Corp., and other analyst groups conduct

independent studies of TCO with numerous clients. These studies provide industry averages for improving various components of IT costs within the enterprise. Although TCO results vary, it is important to understand that these studies and averages only provide a starting point for understanding IT costs. IT professionals adopt or customize a TCO model that fits their unique IT environment.[29] Additionally, GSA is developing a cost-analysis model to aid federal agencies with this process. GSA also has awarded contracts to two consulting firms, Harris Corp. and VGS Inc., to help agencies placing orders under the GSA's Seat Management program described earlier.[30]

TCO analysis should be the first step of an organization considering a seat management program or any other IT outsourcing venture. Data from a TCO study will help an organization determine its current level of service and associated costs. Mr. Paolillo, a Gartner Group executive, stated, "In order to make good IT decisions and maintain your competitiveness, you have to be aware of the total environment in which your information technology is performing. Measurement is the key component in a manager's toolset for driving continuous improvement."[31]

In summary, a TCO analysis may or may not support the decision to ultimately implement a seat management or other outsourcing program, but the analysis itself is still a valuable tool that can assist an organization in making internal improvements.

Chapter 5

The Department of the Navy's Solution – NMCI

Audaces fortuna juvat (Fortune favors the bold)
- Latin Proverb

By this point it should be clear that seat management is a possible method to solve the IT infrastructure problems resident within the Defense Department - problems that stand in the way of the ultimate achievement of information superiority. It is imperative to view outsourcing not as a cure-all solution or a band-aid fix, but as a *tool* to integrate the expertise that resides within the commercial IT industry into the solution. As mentioned in the introductory chapter, the NMCI contract, awarded to Electronic Data Systems (EDS) this past October, is the largest service contract ever awarded in the U.S. government – close to $7 billion. The sheer size and scope of the NMCI project are a tribute to the vision and boldness of the Department of the Navy in confronting the challenges of an uncertain future. This chapter will describe the NMCI project in greater detail, to include discussions concerning the history, mission, and organization of the NMCI; the NMCI transition plan, and the contract management plan. At the conclusion of this Chapter, a brief description of EDS will be offered.

History of the NMCI

NMCI is the culmination of a five-year effort to lay the foundation for a Department of the Navy enterprise network. The central themes described in the earlier chapters of this paper have been commonly echoed throughout the leadership of the Defense Department. According to the former Secretary of Defense, the Honorable William S. Cohen:

> DoD has labored under support systems and business practices that are at least a generation out of step with modern corporate America. DoD support systems and practices that were once state-of-the-art are now antiquated compared with the systems

> and practices in place in the corporate world, while other systems were developed in their own defense-unique culture and have never corresponded with the best business practices of the private sector. This cannot and will not continue.[32]

Furthermore, Dr. Jacques Gansler, the Under Secretary of Defense for Acquisition and Technology states:

> We are facing an unprecedented challenge to modernize our forces in a world that demands more efficient as well as more effective acquisition. To meet that challenge, we are engaged in the Revolution in Business Affairs….To be successful, several changes are needed in DoD's management, business, and technical practices…We all must rededicate ourselves to more aggressive change. We will make mistakes along the way. And we may be criticized for these mistakes, but dramatic effects can only come when we take and manage risks and begin to act more like the competitive commercial sector does.[33]

Recognizing this, the Navy and Marine Corps began efforts to improve network connectivity within their services in 1998. The Marine Corps had initiated the Marine Corps Enterprise Network (MCEN), and the Navy was planning the Navy Wide Intranet (NWI), formerly known as the Navy Virtual Intranet (NVI). However, after discussions held in February 1999 among the DON Chief Information Officer (CIO), the Under Secretary of the Navy and the Assistant Secretaries of the Navy (ASN) for Research, Development, and Acquisition (RDA) and FM, the SECNAV directed that the DON CIO combine MCEN and NWI into one effort. In March 1999, ASN (RDA) further directed the combined efforts be purchased as a service, rather than the DON owning or building anything new. RDA strongly recommended that the DON capitalize on the billions of dollars that the commercial industry was investing in IT rather than DON reinvesting in the same areas.[34]

As explained in Chapter 4, several Federal agencies and much of the commercial sector recently began to acquire IT capabilities through the use of long-term seat management service contracts. "In May 1999, the Department of the Navy decided that the requirements of the NMCI could be satisfied most efficiently and effectively by a single private sector entity

providing end-to-end IT capabilities as a service under a long-term commercial-type 'seat management' contract."[35] This decision was based primarily on:

- The lack of interoperability within the DoN's shore IT infrastructure
- The need to achieve IT interoperability with the Navy and Marine Corps and joint forces
- The ability to quickly and effectively harness the continuing rapid developments in commercial IT
- The demonstrated ability of private sector companies to design and manage enterprise-wide networks through the use of seat management type contracting

Figure 3 is a graphical depiction that describes the current and future network interoperability posture within the DoN.

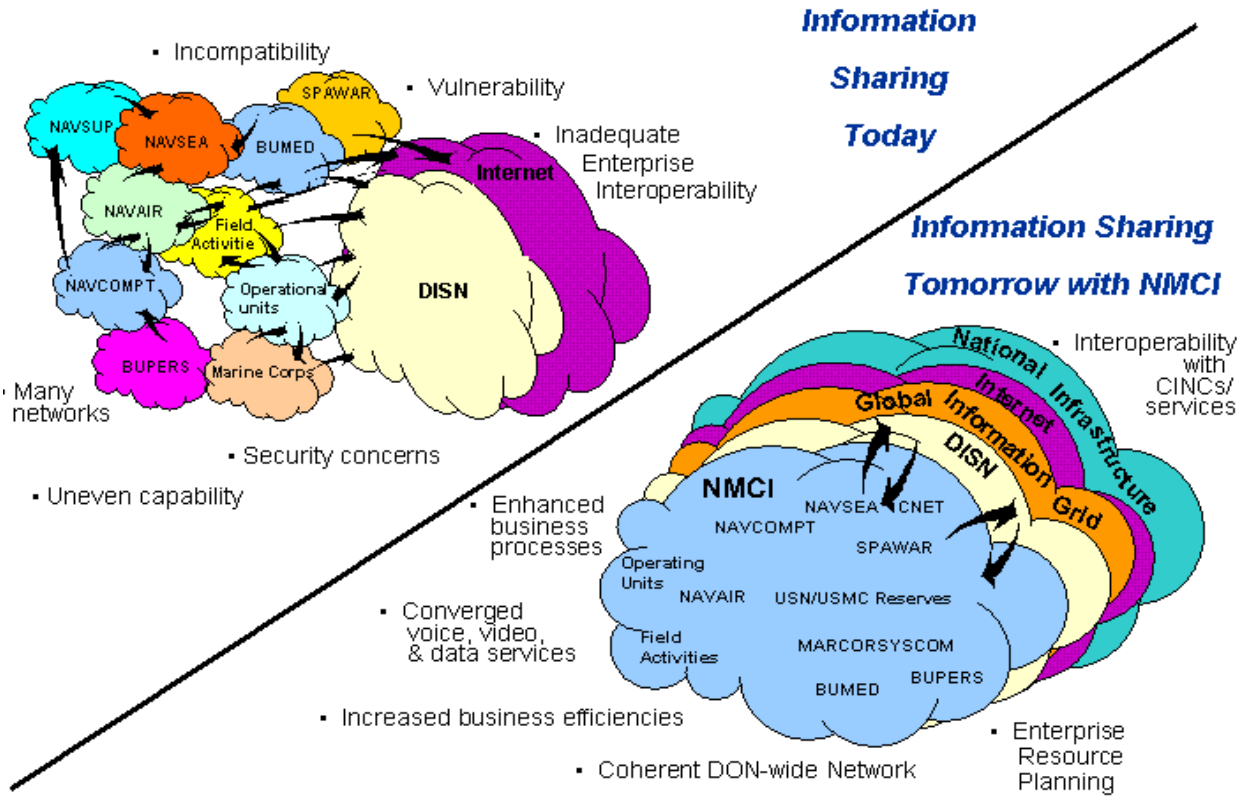

Figure 3: Interoperability Posture[36]

The "end state" (or "to be" environment) envisioned by DON is defined as a

> single enterprise-wide network capability providing end-to-end, secure, assured access to a full range of voice, video, and data services to support both business applications and war fighting missions for all Navy and Marine Corps IT users, including those assigned

to ships and deployable Marine Corps units. The afloat users will be supported by the Information Technology for the 21st Century (IT-21) initiative. All other DON requirements will be provided by the NMCI.[37]

It should be noted that the deployed Marine Corps units will be supported by the Marine Corps Tactical Network (MCTN). Refer to Figure 4.

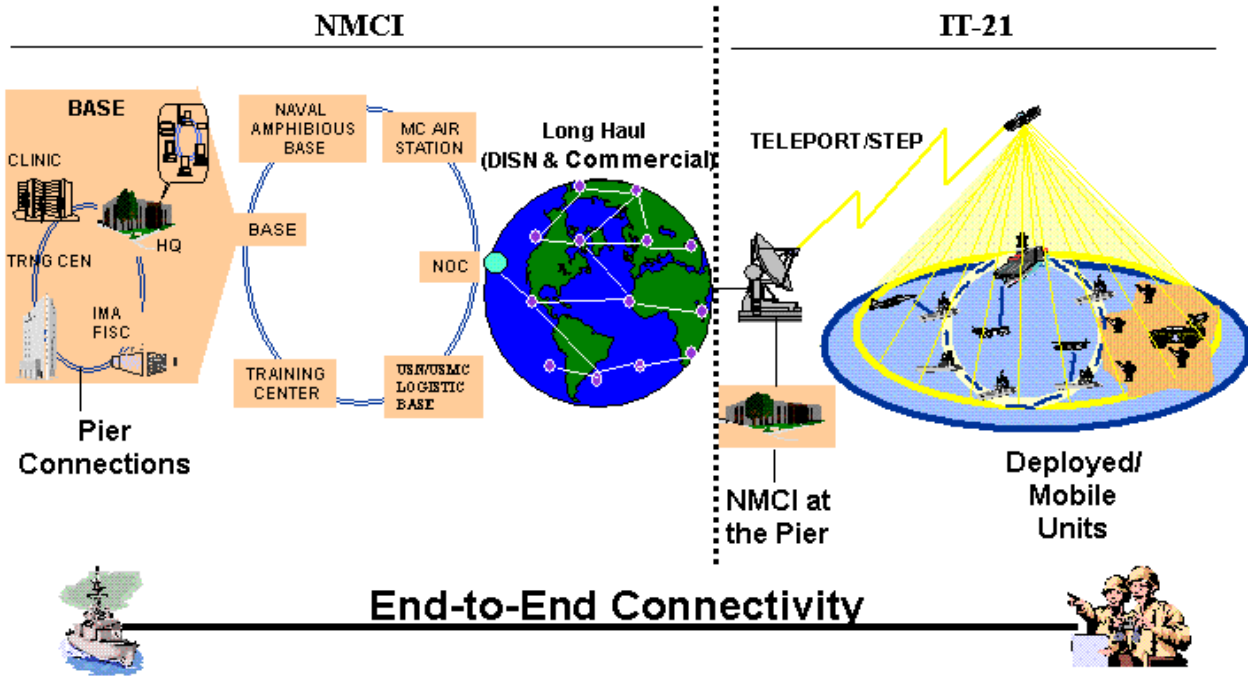

Figure 4: Proposed NMCI Environment[38]

Having now a general understanding of the desired end-state of the NMCI, let us focus our attention to the specific missions and goals. We can then discuss the formal Analysis of Alternatives conducted and the details of the proposed solution.

NMCI Mission/Goals

According to the Navy's NMCI Program Management Office (PMO), the NMCI mission is to plan, coordinate, and align the entire information infrastructure, to include enterprise systems and data under a single, coherent and forward-looking strategy. The information infrastructure must collectively provide to the warfighters and decision-makers the right information at the right place and the right time. Therefore, the NMCI solution and strategy must be aligned with and support a wide range of current and future DoN

initiatives to reengineer business processes and support evolving warfighting operational concepts.[39]

Specific NMCI goals include the following:

- Provide migration from the current DoN IT environment to the NMCI environment with minimal negative impact on current and projected operations
- Provide users adequate capacity and bandwidth as needed with minimum network latency
- Remove access, connectivity, and throughput impediments to productivity and speed of command
- Quickly and securely share knowledge around the globe
- Eliminate interoperability problems
- Align NMCI solutions and strategies to support related initiatives that improve information management
- Reduce cost of voice, data, and video services
- Ensure the implementation strategy provides a continually advancing level of capability and performance
- Ensure the highest level of customer satisfaction through continuous monitoring, rapid resolution of incidents, and technology refreshment to ensure NMCI exceeds evolving demands for service
- Be responsive to evolving security threats[40]

Business Case Analysis

In order to evaluate better the potential cost of the NMCI against a comparable current baseline (TCO), the Navy has performed a Business Case Analysis (BCA). Of particular relevance to the budget estimates, the BCA identified an "as-is" estimate of what the NMCI-like portion of the current DoN IT costs amount to. Absent from such an analysis, the baseline IT infrastructure support cost is indistinguishable within the DoN budget. The as-is BCA identified 335,000 current "seats" (as of FY1999) throughout the DoN and an average annual cost of $4,582 per seat.[41] This baseline pre-NMCI BCA will be compared to post-NMCI BCAs to determine actual savings per seat.

Analysis of Alternatives and Concept Selection

In response to the specific requirements established in the Clinger-Cohen Act described earlier, a formal Analysis of Alternatives was conducted by the Department of the Navy to fully evaluate the NMCI proposal. The three alternatives considered were:

1) Continue with the As-Is environment
2) Government centrally owns and operates WANs, MANs, and BANs through Regional Network Operations Centers. LANs and Desktop hardware/software to be procured by individual commands. All hardware and software purchased using existing contracts. Purchase IT as a *product*.
3) Buy complete IT capabilities as a service under a long-term commercial-type "seat management" contract (contractor owned and operated).[42]

The merits of the alternatives were analyzed in terms of the following attributes:[43]

- Performance
  - Standardization/Interoperability
  - Security/Information Assurance
  - Level of Service
- Cost
  - Seat Cost
  - Feasibility
  - Effectiveness
  - Visibility
- Schedule

A thorough quantitative and qualitative analysis of the alternatives was subsequently conducted that ultimately led to the DON decision to buy the IT capabilities as a service (Alternative #3). This alternative buys as a service everything necessary to ensure seamless, end-to-end transmission of voice, video, and data. It includes associated capital infrastructure improvements necessary to meet quality of service requirements, as well as maintenance, training, and operation of that infrastructure. Under the service contract, the service provider owns and maintains all required desktop and network hardware and software, and provides all required IT services, including pier connectivity (to IT-21/MCTN). In addition, all existing IT infrastructure at the government sites will be provided to the contractor. The service provider

also is responsible for ensuring that the transition from the current operational environment to the enhanced environment takes place without impacting ongoing operations. In summary, the government buys the service on a per seat basis.

Performance. When a customer buys a service, a method for measuring the provider's service must be established. These agreements are called Service Level Agreements (SLAs). The SLAs define the way in which performance will be measured, and gives the customer the right to withhold payment if the service levels are not achieved. Conversely, the provider can also be rewarded for achieving high performance levels. The NMCI is a contract based on SLAs and associated performance measures (which will be discussed in greater detail later in the paper).[44]

Standardization/Interoperability. The service contract specifies the services available as Contract Line Item Numbers (CLINs). The CLINs represent items such as fixed workstation seats, mobile phone seats or moveable VTC. Figure 5 graphically portrays the CLIN seat options within NMCI. Commands will select (buy) these items based on their internal IT requirements and allotted budget ceilings. Thus, a VTC capability at one command on the East Coast is identical to a VTC capability at a separate command on the West Coast. Similarly, all workstations will have the same desktop/network operating systems (e.g., Windows 98/NT) and e-mail systems (e.g., Microsoft Outlook). While the hardware and software infrastructure is the responsibility of the vendor, the government can specify through the SLAs the requirement for interoperability, both within the NMCI and with the rest of DoD. Additionally, the government can require that the vendor conduct interoperability tests for any capability for which interoperability is part of the SLA in order to prove that their solution will

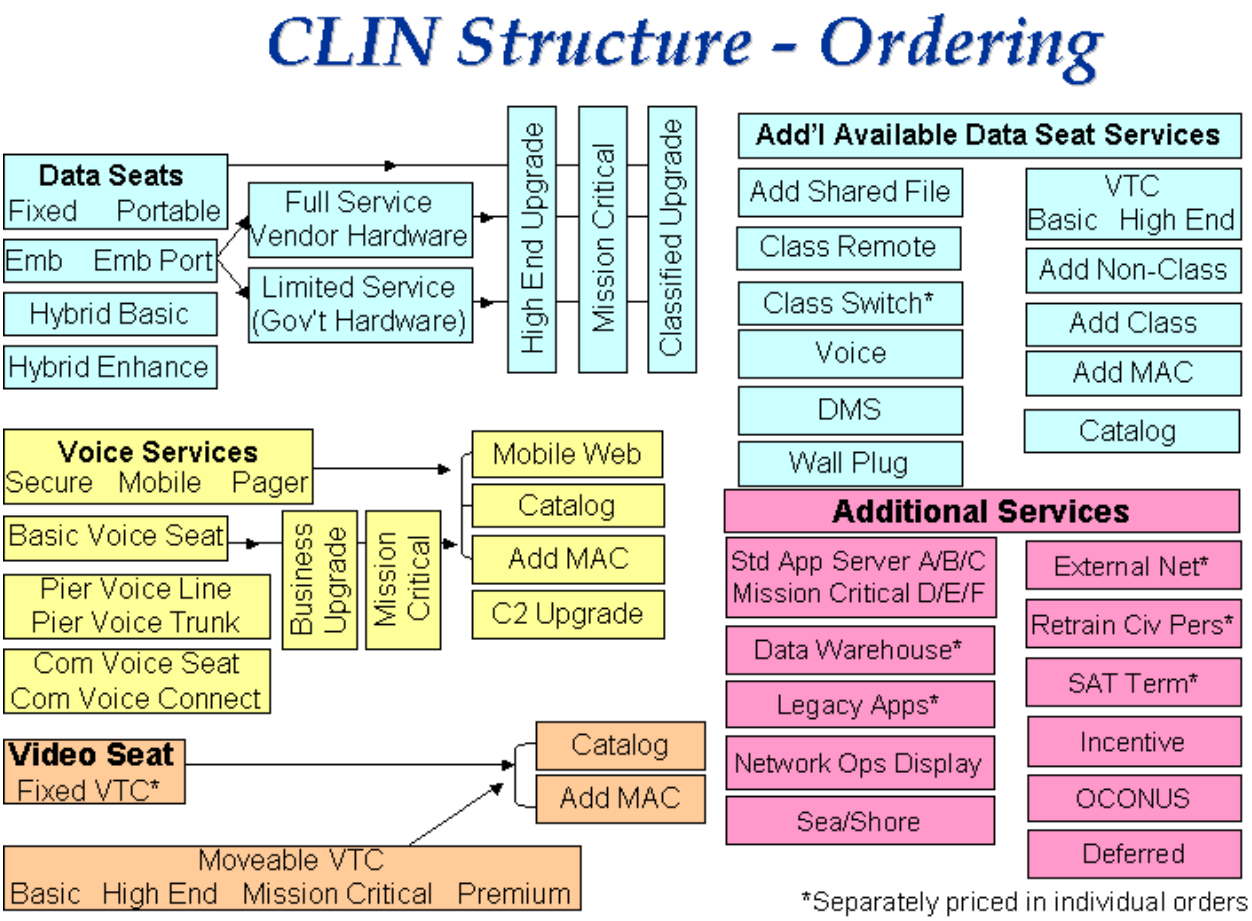

Figure 5: NMCI CLIN Seat Options

be interoperable. As with performance, the government has the option of not paying for the service should any interoperability problems surface. Therefore, the vendor has a great incentive to ensure that all of the system functionality provided is interoperable.[45]

Seat Description and Cost. As mentioned, seat costs will vary according to the options desired. According to the actual NMCI contract, the seat descriptions and their associated costs can be viewed in Appendix A. When comparing the costs associated with a seat management environment, it is important to remember that the entire costs of the IT infrastructure environment are passed down to the seat. In other words, the labor costs of the engineers and administrators working at the network operations centers are included in the seat cost. There is no "overhead" under NMCI. When the contractor submitted his contract terms, he took into

consideration the entire Total Cost of Ownership and the associated number of seats that would be provided. Whether the contractor turns a profit or goes broke is the risk that he takes. Instead of spending billions of dollars into IT overhead, the Navy is using that money to buy hundreds of thousands of seats. It is essential to understand that these seats, which may seem expensive when compared to just the hardware portion alone, include the entire shore-based IT infrastructure of the Department of the Navy. This topic of TCO and seat cost will be discussed further in the next Chapter.

Security/Information Assurance. As described earlier in this paper, industry has been buying IT services through seat management contracts for several years. But since the security requirements of the Department of the Navy are unique compared to private industry, the service contract must be adapted to ensure that the intranet is secure and in compliance with DoD and DoN requirements. Therefore, the contract must stipulate that authorized DoN personnel will perform a number of critical security roles. These roles fall into two categories: (1) ensuring that the security of the intranet satisfies DoN, DoD, and Federal requirements and (2) exercising essential command authority over DoN defensive Information Warfare (IW) activities.[46]

Additionally, in concert with the requirements for Certification and Accreditation of all DoD computer networks (classified and unclassified), authorized DoN personnel will be the approving authority for the following components of the NMCI:

- Security Architecture
- Security critical product selections
- Network connectivity plan
- Security procedures

Beyond that, the government can include SLAs for Security/IA designed to verify that the required IA functionality is being implemented for the intranet. Award fees and other incentives

for successful implementation of key IA functionality (PKI, SIPRNET connectivity) can help ensure that the intranet meets all security/IA requirements.[47]

Level of Service. The NMCI will provide every user within the Navy and Marine Corps enterprise with a consistent level of service that is clearly documented and measurable through SLAs. Additionally, the vendor will refresh hardware and software at required intervals, so no command will be forced to use inadequate or unsupported hardware or software.

NMCI Organization

NMCI Oversight. Due to the complexity of the NMCI project, great emphasis has been placed on its oversight by Congress and the Department of Defense (refer to Figure 6).

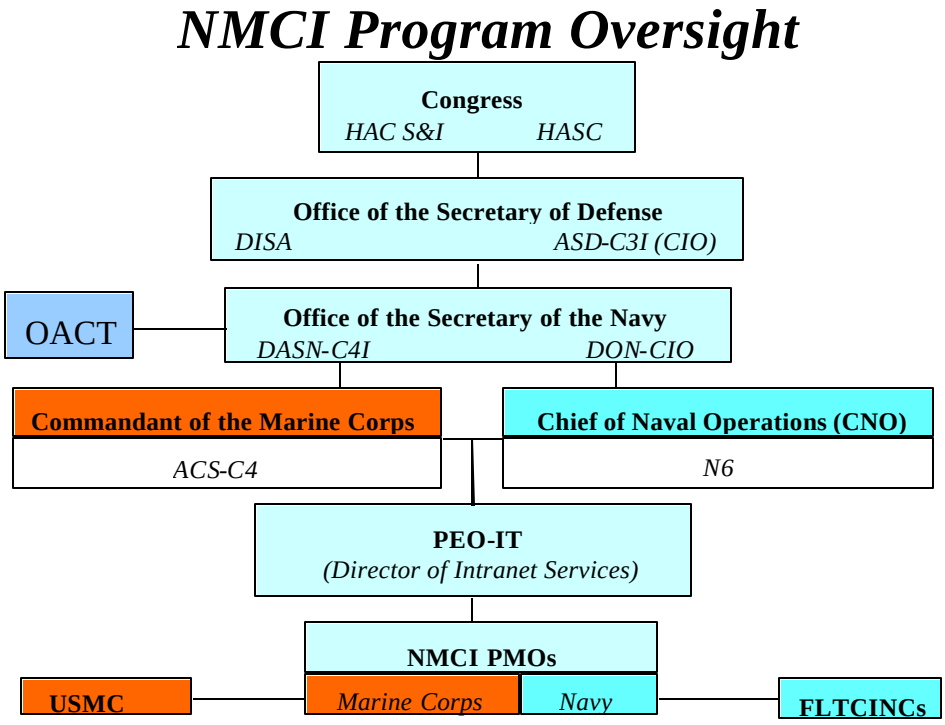

Figure 6: NMCI Program Oversight[48]

Congressional oversight is provided primarily through the House Appropriations Committee Survey and Inspection Team (HAC S&I) and the House Armed Services Committee (HASC).

The Defense Information Systems Agency (DISA) provides assistance and oversight in evaluating NMCI system objectives, reviewing implementation methodology, and reconciling development efforts to DoD IT guidance. DISA administers the Defense Information Systems Network (DISN), which provides connectivity to other DoD and Governmental agency activities. All WAN requirements and long haul services provisioning are monitored by DISA. NMCI interfaces directly with the DISN to transport voice, video, and data.[49]

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I) serves as the DoD CIO. In this capacity, the ASD C3I provides guidance and oversight in leveraging current technology to achieve information superiority and consistency of infrastructure development in support of warfighter requirements. The DoN CIO is responsible for providing oversight for all information management/information technology (IM/IT) strategic developments as it relates to NMCI. Both the ASD C3I and the Deputy Assistant Secretary of the Navy for C4I (DASN C4I) will play important roles setting policy and guidelines in managing the efforts of NMCI.[50]

NMCI Governance. The governance process is responsible for the creation of policy, procedures, standards, and guidelines regarding the NMCI, as well as their currency. The governance process will also review and approve enterprise-wide requirements and resource allocation for the NMCI. The governance process deals with the needs of the enterprise in an open forum called a Stakeholders' Council, and forwards issues for decision, when appropriate, to a decision body called the Executive Council. The members of the Executive Council are the DoN CIO as well as the OPNAV N6 and the HQMC C4. All members of the NMCI Executive Council are members of the DoD CIO Executive Board, which is the DoD Global Information

Grid governing body. The NMCI Executive Council will be a standing organization, meeting as required.[51]

The NMCI Executive Council will coordinate with the PEO-IT, claimants, and SysComs for execution of policy decisions in addition to providing direction to the Commander Task Force NMCI (CTF-NMCI), the operational arm of NMCI. The NMCI Stakeholders' Council will provide input to the NMCI Executive Council on issues that require resolution and decision. The Stakeholders' Council will be composed of representatives from USN and USMC claimants and major commands. The CTF NMCI will chair the Stakeholders' Council. Enterprise Action Groups will work those NMCI issues that require enterprise solutions. These Groups will be staffed with active duty technical personnel from claimants and major commands. Figure 7 below shows the governance relationship.

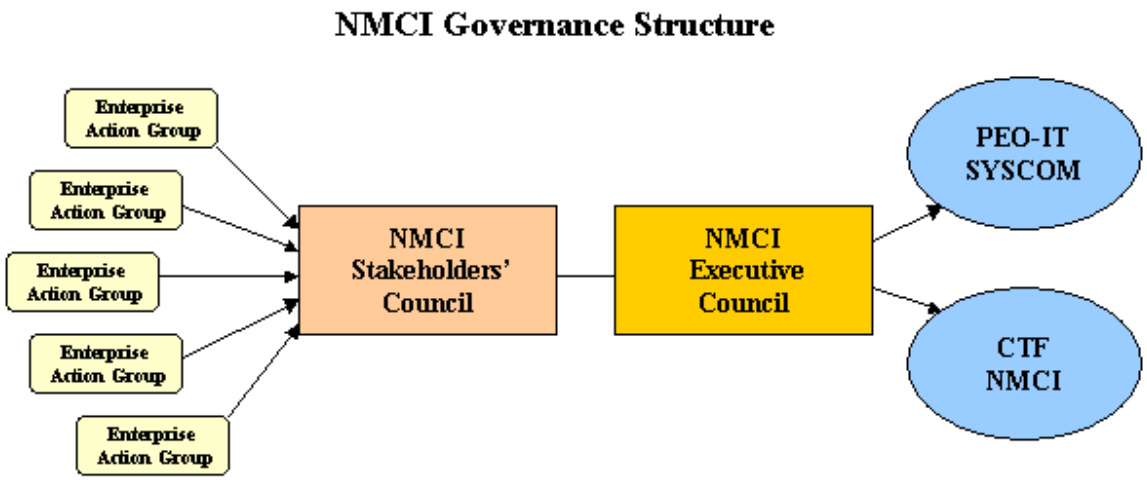

Figure 7: NMCI Governance Structure

NMCI Operational Control. The CTF-NMCI is responsible for the day-to-day operation of the Department of the Navy IT network. The CTF oversees overall performance of the network to ensure reliability, availability, and security of critical information. The CTF is the central point of contact to the NMCI contractor for network operations and coordinates all

decisions involving network support to operations. The CTF is responsible for implementing and monitoring network priorities and policies as directed by the NMCI governance organization. The CTF is also the Designated Approving Authority (DAA) for the NMCI and approves certification and accreditation of the network to operate at an acceptable level of risk. The CTF may establish a presence at the Contractor's global Network Operations Center (NOC) or Network Management Center to monitor overall NMCI operations for the Government. NMCI network management policies, procedures, and tools must enable to Government to exercise operational direction over critical segments of the NMCI infrastructure in support of DoN statutory and warfighting responsibilities. Operational direction includes the ability to set priorities for contracted services and to direct changes in network security posture.[52] The following Figure depicts how operational control will be managed.

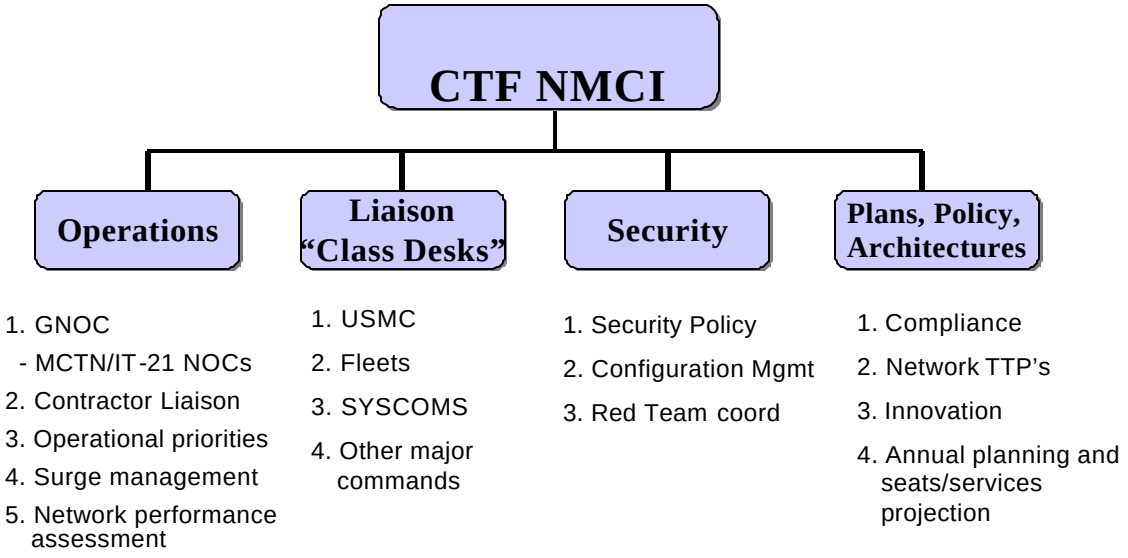

Figure 8: CTF NMCI Organizational Structure[53]

NMCI Contract Execution. To implement the NMCI contract execution strategy, PEO-IT has developed a geographically diverse, decentralized support infrastructure with the PMOs as the program's overall manager. The principal mechanism for implementing NMCI is the

Government Management Offices (GMOs). The four Navy GMOs will support claimant requirements planning, ordering, billing, and contract execution. Locations were selected to support user concentration areas. The highly centralized structure of the Marine Corps lends itself to the formation of a fifth USMC GMO to perform similar functions. The Navy GMOs will report to SPAWAR PMO and interface with SPAWAR Contracting and Comptroller departments. The USMC GMO will report to the USMC PMO. The GMOs will provide technical, contractual, and financial support to ensure the successful execution of the contract.[54]

Within each GMO structure exists a Lead Engineer (LE) and Contracting Officer's Representatives (CORs) to facilitate information flow up and down the organization. The CORs interact with Customer Technical Representatives (CTRs) who translate unit/command requirements to the COR. Figure 9 describes the organizational structure graphically.

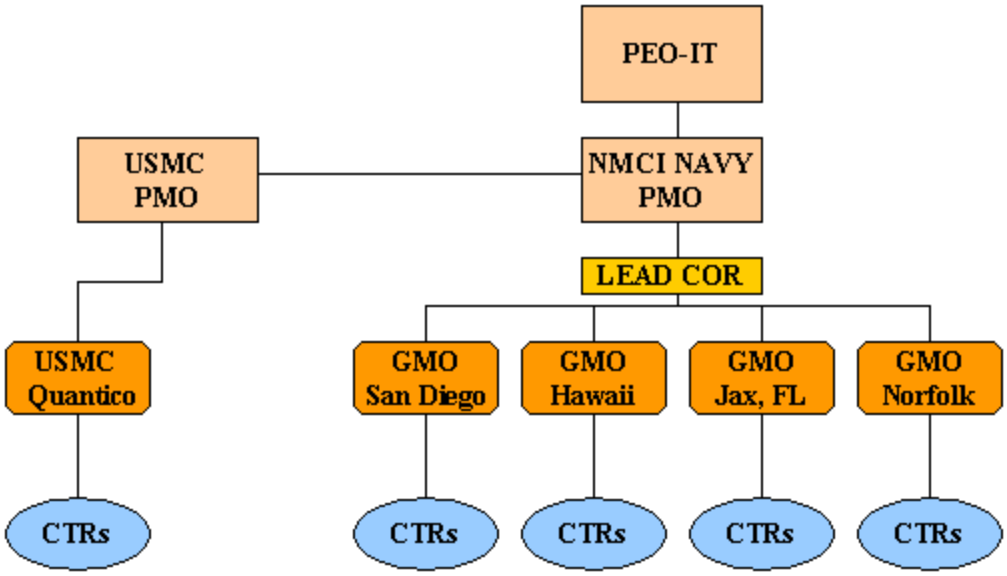

Figure 9: NMCI Government Management Office Structure

It should be understood that the multitude of organizational structures described in the preceding pages are new and are in the process of being instituted. As the Contractor

implements his execution strategy, the governmental structures will probably be adjusted in order to facilitate efficient and effective oversight and control.

NMCI Transition

The overall management approach to transition will involve the CTRs with close coordination of each claimant, command, and activity. The claimants and commands nominate the CTRs based upon the distribution of CONUS commands. The Navy estimates that 94 CTRs will be required to support the CORs at the three Navy GMO locations in Norfolk, Va., Jacksonville, Fl., and San Diego, Ca.[55]

Each activity's transition schedule will depend upon the activity as it relates to the number of seats to be transitioned. For planning purposes, the activity sizes are defined as small, medium, and large.

Table 1: NMCI Activity Size[56]

Activity Size	Number of Seats	Number of Activities
Small	1-9	1200
Medium	10-249	800
Large	249-	400

Essential to supporting the transition process is a Memorandum of Agreement (MOA) which will form the basis of agreement between the Navy/Marine Corps claimants and the NMCI USN PMO/PEO-IT and the USMC PM NMCI. The MOA applies to all units, activities, and sites subordinate to the claimancy and acts as the governing document for the transition of NMCI to the claimant. During the Claimant Planning Phase, the claimant should also define the security policy for physical, personnel, procedural, and COMSEC security and the acceptable level of risk for NMCI operation at the subordinate units. NMCI CMS custodian responsibilities will be addressed within the MOA.[57]

Detailed planning at the activity level will ensure successful implementation of NMCI. To accommodate the tasks necessary and to assist each activity, the Customer Technical Representatives (CTRs) will host a series of meetings to facilitate the activities in transition planning and support. The details concerning the six transition meetings were published in the official NMCI Execution Plan by the Navy and can be viewed in Appendix B.

The following specific activities should be performed by every command in concert with the Contractor and the Contractor's transition plan: appointing a Transition Team; gathering data on the existing IT environment ("as-is"); supporting the Contractor's due diligence period; preparing to place an order for basic services; and understanding the transition process. Preparing for the implementation is the key to a smooth transition. Specific timeframes will vary upon each site's complexity and requirements for physical upgrades (e.g., upgrading substandard network cabling).

Of critical importance in preparation for the transition and implementation is defining the "as-is" environment. The NMCI Transition Data Collection Template and User's Guide has been prepared as a data collection tool for commands to utilize while transitioning to the NMCI services. The template is used to gather such specific information as facilities, key personnel, existing contracts, proposed disposition of existing equipment, physical security, inventory, help desk/technical support, application requirements (legacy and new), database requirements, physical network connectivity, and training.[58]

The Implementation Process/Timeline. The implementation process itself consists of seven steps and is described as providing the support necessary to the Contractor and fully understanding the Contractor's process for transition. These steps consist of:

- Providing government support to the Contractor
- Understanding the Contractor's Process

- Preparing to place an order
- Exiting from existing contracts
- Continued NMCI transition
- Sustainment
- Monitoring IT services

The original NMCI schedule called for contract award in July 00, first increment implementation commencing in the first quarter of FY01, followed by a second quarter strategic pause during which DoD and DoN would conduct a test and evaluation of NMCI to review performance results. That schedule slipped based on the delay in Congressional approval last summer. Approved NMCI deployment since then includes a first increment implementation covering portions of the Naval aviation community (approximately 40,000 seats), followed by testing and evaluation, and finally a DoD review and assessment to determine NMCI suitability for continued implementation.[59] Specific facilities within the Naval aviation community in the first increment include NAVAIR, China Lake Naval Weapons Facility, Point Mugu, CA, and the Washington Naval Yard, to name a few.

The implementation schedule includes: Assumption of Responsibilities (AOR) for the first increment beginning mid-December 2000 to February 2001, test and evaluation for the first increment to be performed beginning in March 2001, and final review and accreditation of the first increment immediately following. The AOR is the date when responsibility for operating the "as-is" environment at a particular facility shifts from the Government to the contractor. As of mid-February 2001, the contractor has already assumed responsibility (through AORs) for approximately 17,000 NMCI seats.[60] According to the Navy, NMCI will take two years to reach its Full Operational Capability (FOC).

Contract Management

As explained earlier, in order to facilitate a new approach largely based on commercial sector practices, unique contract terms and conditions were developed to acquire IT services for the government in a seat management concept. Generally speaking, from a contracting perspective, NMCI is a performance-based, incentive-oriented contract. To assist in achieving the stated objectives, the PEO-IT has built into the NMCI contract four incentive awards for the Contractor:

- A Full Operational Capability (FOC) one time incentive payment
- A customer satisfaction per quarter incentive payment
- An IA biannual incentive award payment
- A small and disadvantaged business participation biannual incentive payment

Additionally, in order to promote customer satisfaction and overall performance of NMCI services, the contract contains clauses in which the Government will receive credit for services that the Contractor fails to provide at the specified requirement or SLA. The payment of some incentives and nonpayment for credits hinges on whether or not the Service Level Agreements have been met. The SLA monitoring is a tool integrally tied to the expected performance of the NMCI services. Should the Contractor meet or exceed those expectations, this will earn him financial reward. However, should he fail to meet those expectations he will lose money.

SPAWAR will be the financial/administrative execution agent for the Navy portion of the contract and MARCORSYSCOM will coordinate all Marine Corps orders. Consequently, the SPAWARSYSCOM Comptroller's Office shall manage all Navy NMCI funding and MARCORSYSCOM will centrally manage NMCI funding for USMC commands and issue its own unique Lines of Appropriation (LOAs). The LOAs and Work Requests (NAVMC 2275) will be forwarded to the appropriate GMO as designated by the governing PMO.[61]

Electronic Data Systems (EDS)

Established in 1962, EDS is a professional services firm that applies consulting, information, and technology in innovative and productive ways to enable clients to improve their overall performance, extend their enterprise ahead of the competition, and better serve their customers. The company's end-to-end services portfolio includes Management Consulting, E-solutions, Business Process Management, and Information Solutions. Each of these areas has tremendous growth potential in the coming years and each contains a wide assortment of related service offerings.[62]

EDS has the reputation of being highly innovative in using technology to solve business problems and help clients in such areas as improving customer service and enhancing the quality of their products. EDS is a recognized global leader in providing E-business and information technology services and has over 9,000 business and government clients in approximately 55 countries around the world. The company has more than 121,000 employees worldwide. The company is very strong financially with registered revenues of $18.53 billion in 1999 and new contracts totaling over $24.9 billion.[63]

Chapter 6

Analysis of the NMCI Project

The NMCI project has been the subject of significant debate throughout the Navy and the Marine Corps since its inception. The evidence suggests that there are two differing schools of thought concerning NMCI – the USN perspective and the Marine Corps perspective. While most would agree with the general "concepts" described thus far in this paper, the general feeling within the Marine Corps is that the NMCI is unnecessary – owing mostly to the fact that the Marine Corps Enterprise Network (MCEN) was already fully modernized and interoperable within the GIG and the Joint community. One must keep in mind that the Marine Corps' portion of the NMCI project is quite small (less than 20%) as compared to that of the Navy's. The Marine Corps was not given the opportunity to refuse participation within NMCI, but was forced by the SECNAV to migrate along with the Navy. The biggest complaint by the Marine Corps (unofficially) is the fact that the Navy is scouring all Navy and Marine Corps IT infrastructure and IT related programs to recover funding which will be used to pay for the NMCI. These funding realignments put a severe strain on numerous Marine Corps IT modernization initiatives which will now have to be reprogrammed or scrapped altogether.

Setting aside the intra-Department (Navy) debate surrounding the utility of the NMCI project, this Chapter will address the inherent benefits, risks, and critical concerns of the NMCI from an objective standpoint.

Benefits

Implementation of the NMCI offers the potential of realizing the following benefits:

- True realization of actual TCO vice "best guess"
- Better accounting for IT costs within DoN
- Asset Management

- Security
- "Reachback" Ability
- Cost effective (economy of scale)
- Faster Refresh Rate
- Enterprise-wide standardization

Actual TCO. With the implementation of the NMCI, the actual TCO for the entire Navy and Marine Corps can finally be defined. Prior to the Business Case Analysis conducted last year in preparation for the NMCI, there were no concrete figures for the total cost of the Navy and Marine Corps IT infrastructure. Even the Business Case Analysis is a "best guess," the results of which are subjective. Once the NMCI Final Operational Capability (FOC) has been achieved, both the contractor and the Navy will be able to provide an exact accounting for all costs associated with the NMCI. This will at least give the US Navy and Marine Corps a firm handle on its shore-based IT infrastructure requirements and costs. With an actual TCO established, the Navy and Marine Corps can more effectively and efficiently program future funding for IT requirements.

Better IT Cost Accounting. With centralized accounting control administered between EDS, SPAWAR, and MARCORSYSCOM, true cost accounting can be conducted for budgetary and managerial purposes. Along with the actual TCO described above, this should satisfy any inquiry concerning where and how the Department of the Navy spends its money on IT infrastructure.

Asset Management. EDS will be utilizing the latest inventory control technology to maintain 100% accountability of all hardware, software, and infrastructure used within NMCI. Currently, neither the Navy nor the Marine Corps could produce a report describing how many Pentium III computers it currently has on hand. A centralized, modern asset management capability will be utilized with the NMCI.

Security. Without going into technical detail, intranets (as opposed to extranets) are inherently more secure by design. Bringing all of the networks of the Navy together with the MCEN into a single intranet will drastically reduce the Point of Presence (POP) requirements and will allow for better internal and external security measures to be implemented and controlled. This will allow for better information assurance and computer network defense (CND).

To better understand the fundamentals of intranets, consider the following analogy. Imagine each of the hundreds of sovereign nations of the world as independent networks. The aggregate total of all the global countries (networks) correspond to the internet as we know it. Millions of people (data packets) routinely travel from nation to nation each day, with relative ease. Now let us take a closer look at the continental United States and associate it as a singular intranet within the global internet, even though each of the 50 states represents independent networks themselves. From a security perspective, the physical borders of the United States represent the physical borders of the intranet. The principal entry points into the United States are through its international airports and seaports. Similarly, the entry points into an intranet are through physical connections known as Points of Presence (POP). As our airports are guarded by the U.S. Border Patrol, intranets are guarded by "firewalls." For people to enter the United States, they must possess appropriate documentation (a valid passport or visa). For data to enter an intranet through a firewall, it must also contain the appropriate access documentation (correct address, access control, etc). As the Border Patrol allows only authorized persons to enter the United States, a firewall allows only authorized data packets to enter the intranet. Once inside the United States, people have the freedom to move among the different states. Similarly, once inside the intranet, packets are free to move from network to network without having to pass

through internal firewalls. In summary, you can see from this analogy that one, tightly controlled intranet with a hundred POPs is easier to secure than many independent networks with thousands of POPs.

Reachback Ability. Conceptually, the NMCI will allow for better interoperability between the shore-based NMCI and the deployed (afloat) forces utilizing the IT-21/MCTN via the STEP interfaces. As an example, the 15th MEU Operations Officer on board the *USS Bonhomme Richard* off the coast of Africa will be able to tap into the training databases at the MAGTFTC in 29 Palms, CA to retrieve information vital to a current operation. The main constraint to possessing this reachback capability is the bandwidth requirements needed to facilitate it. Through our technological innovation, we have engineered a truly global network. However, the data still have to pass through numerous types of physical mediums (copper, fiber optic cable, air) and multiple connections (routers, switches, CSU/DSUs, etc) to reach their ultimate target. Each individual medium and connection (or node) has its own physical limitations in regards to its throughput capability. Simply put, the larger the throughput, the larger the available bandwidth. Bottlenecks of data quickly form when a node or segment of cable becomes saturated with data coming or going. We've all experienced the frustration of a computer-generated "timed out" error message – most often caused by a bottleneck somewhere downstream. With all NMCI users possessing the capability to "reachback," bandwidth saturation will quickly become an issue. More bandwidth is almost always available – for a price.

Cost effectiveness. In recent years, the DoN has spent an estimated $1.6 billion annually on distributed computing information services and connectivity for CONUS. The NMCI contract will allow the DoN to achieve significant economies of scale by purchasing IT

services form a single entity, thus capitalizing on an enterprise aggregation of services. Estimated costs under the NMCI contract are $1.2 billion annually, representing a significant potential savings to the Government.[64] Just how cost effective NMCI will actually be over the course of the 5-year contract will remain to be seen.

Faster refresh rate. Since the NMCI will be centrally managed, the task of implementing periodic technology "refreshes," or modernizations, throughout the enterprise will be drastically easier to accomplish than before. An example of a technology refresh would be the addition of new anti-virus software, faster CPUs, or more memory for all PCs within the intranet. Current technology refresh rates within the DoN average between 3-5 years per cycle. NMCI could lower that cycle time to as little as 2 years, funding permitting.

Enterprise-wide standardization. Along with a faster refresh rate, a centrally managed intranet possesses the capability to enforce hardware/software standardizations across the entire enterprise.

Risks

The following risks are associated with the implementation of the NMCI:

- Interoperability with existing legacy systems
- Executive/Legislative Interference
- Disruption of service during implementation
- Contractor control of military IT infrastructure

Interoperability with legacy systems. There is little doubt that the NMCI will improve the overall DoN communications posture and force the interoperability of the separate network infrastructures. However, many of the existing legacy systems currently in use will not be easily integrated into the NMCI. Depending on the complexity of the software and/or the age of the programming language, the Navy may have to commit significant funding into either re-

engineering each legacy system or scrapping them altogether if they cannot be modified. On a positive note, the NMCI will force the consolidation and modernization of literally thousands of outdated legacy systems. The NMCI contract has included a split incentive whereby both the government and the contractor receive an award for every legacy system that is replaced or eliminated. This topic will be discussed further as a "critical concern" later in this paper.

Executive/Legislative Interference. A significant risk to the project is the fact that Congress could “pull the plug” at any time if they are not fully satisfied with the results of the NMCI in comparison to its original claims. Congress has displayed significant interest in the NMCI project thus far – particularly in regard to its cost. Congress has demanded a detailed analysis of the NMCI proposal from the Government Accounting Office (GAO). The first GAO report pointed out numerous faults with the original NMCI proposal and made numerous recommendations. Congress would not allow the Navy to proceed with the NMCI project until the Navy addressed the particular concerns – the largest being NMCI oversight and governance. After the Navy had addressed the issues in depth, the GAO, in its second report, gave the Navy “thumbs up”. Even the Office of Management and Budget (OMB) thoroughly reviewed the proposal and the pending NMCI contract. OMB finally approved the project on September 12, 2000 subject to compliance with certain conditions (mostly cost-related). Congress has stated to the Navy that it cannot proceed with full implementation until an analysis of the test case (NAVAIR) is conducted during early 2001.

Disruption of service during implementation. Even though the NMCI project managers are stating that there will be no disruption of service during implementation, the potential does exist for unscheduled network outages. During the full implementation of the NMCI, many network segments will require significant re-engineering in order to meet the SLA

parameters. As LAN segments are optimized, breaks in service will occur. However, once fully implemented, the NMCI should prove quite reliable. The report from the first increment implementation (NAVAIR) in mid-2001 should offer detailed information in this regard.

Contractor control of military IT infrastructure. Any organization, particularly the military in this case, that passes control of an organic function to an external agency automatically inherits the inescapable risk that the external agency will fail to perform. The real question comes down to how much risk is involved and how can the organization minimize that risk to an acceptable level. During the formative stages of the NMCI, the concept of turning over control of the Navy's shore-based IT networks to a contractor raised significant concern. The Navy, realizing the sensitivity of the issue, has built into the NMCI project a robust oversight structure – thereby mitigating the performance risks to a manageable level.

Critical Concerns

Having thus mentioned the benefits and risks of the NMCI project, the following are critical concerns that need to be addressed during the full implementation:

- Initial Seat Purchase at the Unit level (Requirements-Based or Cost-Based?)
- Integration with legacy systems
- Deployability for the Marine Corps
- Displaced personnel
- Governance

Initial Seat Order at the Unit Level. Since the IT requirements vary from unit to unit (and from service to service for that matter), there is reason to believe that an issue will develop during the transition period concerning the determination of initial seat orders. The cursory surveys conducted by the vendors of various Bases and Stations during the Due Diligence period were a poor representation of actual seat requirements. Evidence suggests that these surveys were grossly underestimated. Now if the initial seat orders for units are accepted by the

respective GMOs/PMOs based on the actual IT requirements for that particular unit, then there should be no problem. However, if a "cost ceiling" or "seat # cap" is put in place at the unit level and commanders have to prioritize which seats get purchased against that unit's respective requirements (e.g., the Marine Corps can only afford to buy 100 seats for unit XX when that unit is used to having 110 workstations to support its IT requirements), commanders may believe that the NMCI is negatively impacting their ability to perform their mission. Unit commanders at the tactical level will be scrutinizing very closely at the types of "premium" seats purchased at the higher headquarters levels. Recall from the price breakdown of the seats in the previous Chapter that a "loaded" workstation is oftentimes three to four times more costly than a standard one. What that means is that for every O-6 working at HQMC with a high-end model, four E-4 supply clerks may have to give up their workstations. In summary, there won't be enough money for everyone to get all the "extras" they want. The first year of the implementation will prove difficult for many commands that are IT-intensive, especially units within the supporting establishment since their requirements traditionally take a back seat to the those of the operating forces (for obvious reasons).

Integration with legacy systems. According to the Navy, this concern is one of the largest to confront. The NMCI contract calls for all current legacy applications to be provided full access to the network. EDS and the Navy's Program Office have established a process for laboratory certification of legacy applications working in a Windows 2000 environment. As mentioned earlier, some legacy systems will never make the transition and will be summarily discarded. The Program Office and the vendor have worked out a process in which an accurate inventory of all Navy and Marine Corps legacy applications is made, prioritized, and certified.

Deployability for the Marine Corps. As long as MARCORSYSCOM continues to receive funding and continues fielding tactical, deployable computer assets for the Marine Corps, there is no issue. However, if that funding dries up and gets rolled into the NMCI, Marine Corps units will have to buy deployable seats from NMCI. While these seats will be interoperable with IT-21 and the MCTN, cost may preclude sufficient quantities to effectively allow the Marine Corps to perform its warfighting role. Imagine the I Marine Expeditionary Force deploying to Iraq to fight Desert Storm II with contractor-owned computers. What happens when they break or are destroyed in combat? Who is financially liable for the contractor-owned equipment in a combat zone? Specific procedures and policies need to be implemented to address these issues, especially since this directly affects the Marine Corps' warfighting capabilities.

Displaced Personnel. The Marines and sailors currently filling IT infrastructure billets will ultimately return to the operating forces. The changes to the force structure resulting from the NMCI are currently being studied. The displaced civilians have been offered several alternatives to include relocation to other government agencies/facilities, transitioning to EDS, or being retrained altogether. In fact, EDS has offered to hire any government civilian IT employees displaced by NMCI and provide them work for at least 3 years with a 15% increase in salary. EDS is asking claimants to leave current IT workers on-board after their AOR of the "as-is" network to facilitate a smooth transition. For commands being serviced by IT contractors, EDS is buying out their contracts and taking over the management of their contracts. For networks operated by sailors and Marines, EDS will bring in an augmented work force to facilitate the transition while the sailors and Marines are reassigned.

Governance. Sufficient oversight and governance seem to have been built into the NMCI. However, the multiple hierarchies are complex and seemingly bureaucratic. As full

implementation comes to fruition over the next year or so, the governance structure will be closely monitored by the DoN to ensure the effectiveness of its structure.

Chapter 7

Conclusions

Based on the evidence available, it appears that outsourcing has been very successful in both commercial and governmental ventures to date. While the concept of IT services outsourcing and seat management are relatively new, I can conclude that the probable benefits that could be realized outweigh the potential risks. As previously mentioned, the NMCI is not a panacea – it will not solve all of the Navy or Marine Corps IT issues, particularly since the current infrastructure has been rather reliable, albeit inefficient and costly. The transition will be quite challenging and frustrating at times, especially in terms of cost. In the long run, however, the Navy and the Marine Corps' ability to interoperate and interface with other joint systems will be worth the difficulties experienced in the short term.

The evidence suggests that the critical concerns mentioned in the previous Chapter are indeed significant. However, it also appears that both the DoN and EDS have already established a solid foundation of coordination and cooperation in regards to resolving many of the concerns. As long as this "unity of effort" is focused towards the betterment of the NMCI, I predict tremendous success for this project and similar DoD ventures.

Glossary

ASN	Assistant Secretary of the Navy
ATF	Bureau of Alcohol, Tobacco, and Firearms
BCA	Business Case Analysis
CCA	Clinger-Cohen Act
CIO	Chief Information Officer
CJCS	Chairman Joint Chiefs of Staff
CLIN	Contract Line Item Number
COTS	Commercial Off The Shelf
COR	Contracting Officer's Representative
CTF	Commander Task Force'
CTR	Customer Technical Representative
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DoN	Department of the Navy
EDS	Electronic Data Systems
FASA	Federal Acquisition Streamlining Act
FEDCAC	Federal Computer Acquisition Center
FOC	Full Operational Capability
GCCS	Global Command and Control System
GIG	Global Information Grid
GMO	Government Management Office
GO/GO	Government-Owned/Government-Operated
GPRA	Government Performance Results Act
GSA	General Services Administration
HAC	House Appropriations Committee
HASC	House Armed Services Committee
IA	Information Assurance
IDIQ	Indefinite Delivery/Indefinite Quantity
IO	Information Operations
IOC	Initial Operating Capability
IT	Information Technology
IT-21	Information Technology for the 21st Century
ITMRA	Information Technology Management Reform Act
IW	Information Warfare
JFRG II	Joint Forces Requirements Generator II
JSTARS	Joint Surveillance Target Attack Radar System
JV2020	Joint Vision 2020
KM	Knowledge Management
LAN	Local Area Network
LOA	Line of Appropriation
LogCAP	Logistics Civilian Augmentation Program
MAN	Metropolitan Area Network
MCEN	Marine Corps Enterprise Network

MCTN	Marine Corps Tactical Network
MOA	Memorandum of Agreement
MOOTW	Military Operations Other Than War
NIPRNET	Non-secret Internet Protocol Routed Network
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NVI	Navy Virtual Intranet
NWI	Navy Wide Intranet
ODIN	Outsourcing Desktop Initiative for NASA
OFPP	Office of Federal Procurement Policy
PEO-IT	Program Executive Office for Information Technology
PMO	Program Management Office
RDA	Research, Development, and Acquisition
SECNAV	Secretary of the Navy
SIPRNET	Secret Internet Protocol Routed Network
SLA	Service Level Agreement
TCO	Total Cost of Ownership
VTC	Video Teleconferencing
WAN	Wide Area Network

Appendix A

NMCI Seat Description and Costs

CLIN	Seat Type	Seat Description	Cost/Month
0001AA	Fixed Workstation	Desktop service composed of basic IT characteristics including standard hardware/software, file share service, maintenance, network access, refreshment, administration, customer support, and training	$246.51
0002	Portable Seat (laptop/notebook)	Meets all characteristics of a fixed seat but also provides capability for portable computing	$308.25
0003AA	Embarkable Workstation	Same basic services as a fixed seat but will be periodically deployed and used in an expeditionary or field environment where the workstation will be subjected to rough handling and climactic extremes. Capable of interfacing with IT-21 and MCTN	$468.50
0004AA	Embarkable Portable Seat	Same basic services as a portable seat but will be periodically deployed as described in 0003 above	$375.83
0005AA	Basic Hybrid Seat	Provides access to NMCI environment for users with workstations *not* provided by the Contractor. This is the cost of government-owned PCs/laptops accessing NMCI	$193.11
0006	Wall Plug Service	This service is an *additional* LAN drop beyond those provided with data seat orders. Allows flexibility for internal relocation of registered users/seats to meet surge requirements	$60.00
0007	High-End Seat Upgrade Package	Adds enhanced performance (i.e., high bandwidth and CPU-intensive processing) beyond the requirements of a basic seat	+$204.67

CLIN	Seat Type	Seat Description	Cost/Month
0008	Mission-Critical Seat Upgrade	Adds enhanced availability, reduced network loading, greater maintenance responsiveness	+$182.24
0009	Classified Connectivity Upgrade	Provides classified connectivity including necessary security upgrades to support a secure workstation environment. Used For SIPRNET access.	+$252.17
0010AA	Basic Voice Seat	Provides non-secure telephone-related connectivity including call forwarding, call transfer, call hold, call waiting, call pickup, and hunt group. Includes unlimited local PSTN access and unlimited calls to NMCI voice seats. Does not include toll calls associated with FTS-2001 or commercial long distance carriers.	$45.96
0010AB	Business Voice Upgrade Package	Same as Basic Voice Seat plus voice mail, caller-id, and conference calling	+$10.01
0010AC	Mission Critical Voice Upgrade	Increases availability of service	+$7.68
0011	Secure Voice Seat	Provides user access to secure voice communications services and infrastructure (i.e., STU, STE)	$51.08
0012	Mobile Phone Seat	Provides the user mobile (analog/digital) non-secured voice communication within the NMCI service area. Includes 500 minutes/month with no roaming or long distance charges.	$66.59
0013	Personal Paging Service	Provides non-secured voice and text messages throughout NMCI service area	$33.73
0015AA	Basic Moveable Video Teleconferencing Seat	Provides audio-visual services where users can initiate and participate in live video teleconferencing. Some features include room cameras with full area coverage, large monitors, and dynamic speaker control	$1071.40
0015AD	Premium Moveable VTC Service	Provides 768 Kpbs/30fps quality video and supporting bandwidth	$2061.80

Appendix B

Details of NMCI Transition Meeting

Meeting #1 – Preparation Briefing *(Chaired by the CTR)*

- Discussion of the transition schedule for the activity
- Discussion of CLINs and ordering services
- Introduction to the Data Collection Template and the User's Guide
- Identification of any issues or concerns unique to the activity

Meeting #2 – Preparation Status Meeting *(Chaired by the CTR)*

- Discussion of roles and responsibilities
- The Contractor's transition process
- Review the Data Collection Template and any issues
- Identification of infrastructure requirements
- Identification of physical needs
- Review of the SLAs and user expectations
- Discussion of lessons learned from other activities transition

Meeting #3 – Contractor In-Brief *(This meeting should be geared towards the Contractor and their transition team)*

- Introductions to the Contractor team
- Introduction to the Activity Transition team
- Contractor led discussion on the process, milestones, and schedule
- Establishment of a Transition Baseline
- Creation of a site-specific implementation plan

Meeting #4 – Transition Status Review *(In-Progress Review between Activity and Contractor)*

- In-progress review by the Contractor
- Problem review and resolution
- Schedule to completion review

Meeting #5 – Finalize Order for Activity *(Should focus on finalizing the order for basic seats and services for the activity)*

- Answer questions on the CLIN items
- Compare inventories with the baseline
- Review any changes to the baseline

Meeting #6 – Out-Brief *(Close out of any outstanding issues)*

- Review of outstanding issues
- Generation of lessons learned
- Discussion on the process of ordering additional services

Notes

[1] CAPT William Bry USN, "Navy Marine Corps Intranet (NMCI)," 13 June 2000, URL: < http://cno-n6.hq.navy.mil/n6conf_jun00_archives/n6conf2000files/mf/13/04_nmci-bry/nmci_bry_n6conf_0006.ppt>, accessed 10 October 2000.

[2] *Joint Vision 2020*, (Washington, DC: US Government Printing Office, June 2000),1. Cited hereafter *JV2020*.

[3] *JV2020*, 1.

[4] *JV2020*, 3.

[5] *JV2020*, 8.

[6] *JV2020*, 8.

[7]Dave Bennet, (Dynamic Systems, Inc, sponsored by ARO, ASN(RDA)), "Knowledge Management terms," URL: < http://www.don-imit.navy.mil/textversion/basicSearch.asp?sSearch=knowledge%20management>, accessed 5 December 2000.

[8] Bennet, "Knowledge Management terms."

[9] Department of the Navy Information Management & Information Technology (DON IM/IT) Pamphlet, *Catalog of DON IM/IT Strategic Goals, Tools, and Training* (n.p., July 2000), 9.

[10] Joint Chiefs of Staff, Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: GPO, 10 June 1998), 223.

[11] Joint Chiefs of Staff, Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: GPO, 10 June 1998), 223.

[12] *JV2020*, 28.

[13] *JV2020*, 9.

[14] Gerald J. Ormerod, "Outsourced Logistics: Maximizing External Support," *Marine Corps Gazette*, Volume 81, Number 12, December 1997, 49.

[15] Jerome S. Gabig, "Privatization: A Coming Wave for Federal Information Technology Requirements", *National Contract Management Journal*, Volume 27, Issue 1, 1996, quoting J. Collins and R. Millen, "Information systems Outsourcing by Large American firms: Choices and Impacts", *Information Resources Management Journal*, Winter, 1995.

[16] James A. Dobkins, "Federal Privatization and Outsourcing of Information Technology Functions: A Practitioner's Perspective," *Federal Contracts Report*, Vol. 66, No. 19, Nov 18, 1996.

[17] Office of Management and Budget (OMB), *Circular A-76 Supplement: Part I, Policy Implementation*, URL: <http://www.a76.com/refs/a076s1.html>, accessed 6 September 2000.

[18] Department of the Navy (Interim Guidance), "Information Management/Information Technology Inherently Governmental Functions," 19 April 2000.

[19] General Services Administration (GSA) White Paper, "Outsourcing Information Technology," (February 1998), URL: <http://www.a76.com/refs/finalout.html>, accessed 7 September 2000, 9.

[20] David N. Rasmussen and Keith L. Ruegger, "A Functional Analysis of DOD Implementation of Seat Management," Naval Postgraduate School, Monterey, CA, September 1999, 11.

[21] Federal Computer Acquisition Center (FEDCAC), "Seat Management Overview," (12 July 2000), URL: <http://fedcac.gsa.gov/seat.stm>, accessed 7 September 2000. Cited hereafter as FEDCAC.

[22] FEDCAC.

[23] Rasmussen and Ruegger, 11.

[24] Rasmussen and Ruegger, 11.

[25] Heather Hayes, "Developing a Seat Management Strategy," *Federal Computer Weekly*, 24 August 1998, URL: <http://208.201.97.5/ref/hottopics/seatmgmt/feat1.htm>, accessed 17 September 2000.

[26] Brian Robinson, "NASA JPL:A Seat Management Pioneer," *Federal Computer Weekly*, 24 August 1998, URL: <http://208.201.97.5/ref/hottopics/seatmgmt/feat1.htm>, accessed 17 September 2000.

[27] Rasmussen and Ruegger, 49.

[28] Rasmussen and Ruegger, 49.

[29] Rasmussen and Ruegger, 17.

[30] Hayes.

[31] Rasmussen and Ruegger, 20.

[32] Department of the Navy, "Analysis of Alternatives", *Navy Marine Corps Intranet (NMCI) Report to Congress* (n.p., Washington D.C. 30 June 2000), D-7-1. Cited hereafter as "Analysis of Alternatives".

[33] "Analysis of Alternatives," D-7-1.

[34] "Analysis of Alternatives," D-7-1.

[35] "Analysis of Alternatives," D-7-2.

[36] Bry, "Navy Marine Corps Intranet (NMCI)."

[37] "Analysis of Alternatives," D-7-2.

[38] Bry, "Navy Marine Corps Intranet (NMCI)."

[39] Space and Naval Warfare Systems Command (SPAWAR) and NMCI Program Management Office (PMO), Department of the Navy, *Navy Marine Corps Intranet (NMCI) Execution Plan* (Washington DC, 13 September 2000), 1-2. Cited hereafter as *NMCI Execution Plan*.

[40] *NMCI Execution Plan*, 1-3.

[41] Department of the Navy, "Executive Summary," *Navy Marine Corps Intranet (NMCI) Report to Congress* (Washington DC, 30 June 2000),A-2.

[42] "Analysis of Alternatives," D-7-3.

[43] "Analysis of Alternatives," D-7-3.

[44] "Analysis of Alternatives," D-7-12.

[45] "Analysis of Alternatives," D-7-12.

[46] "Analysis of Alternatives," D-7-12.

[47] "Analysis of Alternatives," D-7-13.

[48] *NMCI Execution Plan*, 2-2.

[49] *NMCI Execution Plan*, 2-2.

[50] *NMCI Execution Plan*, 2-3.

[51] *NMCI Execution Plan*.

[52] *NMCI Execution Plan*, 2-5.

[53] *NMCI Execution Plan*, 2-5.

[54] *NMCI Execution Plan*, 2-15.

[55] *NMCI Execution Plan*.

[56] *NMCI Execution Plan*, 3-1.

[57] *NMCI Execution Plan*, 3-1.

[58] *NMCI Execution Plan*, 3-5.

[59] Deputy Assistant to the Secretary of the Navy for C4I/EW/Space, *Navy Marine Corps Intranet (NMCI) Execution*, 19 December 2000, 1.

[60] Rick Rosenburg, "*Executive Message: NMCI Well Under Way*, URL: http:<www.eds.com/nmci/exec_message_013101.htm>, viewed 17 February 2001.

[61] *NMCI Execution Plan*, 4-10.

[62] "About EDS," URL: <http://www.eds.com/about_eds/en_about_eds.shtml>, viewed 7 January 2001.

[63] "About EDS," URL: <http://www.eds.com/about_eds/en_about_eds.shtml>, viewed 7 January 2001.

[64] Deputy Assistant to the Secretary of the Navy for C4I/EW/Space, *Navy Marine Corps Intranet (NMCI) Execution*, 19 December 2000, 1.

Bibliography

Bennet, Dave. (Dynamic Systems, Inc, sponsored by ARO, ASN(RDA)). "Knowledge Management terms." URL: < http://www.don-imit.navy.mil/textversion/basicSearch.asp?sSearch=knowledge%20management>. accessed 5 December 2000.

Bry, CAPT William USN. "Navy Marine Corps Intranet (NMCI)." 13 June 2000. URL: < http://cno-n6.hq.navy.mil/n6conf_jun00_archives/n6conf2000files/mf/13/04_nmci-bry/nmci_bry_n6conf_0006.ppt>. accessed 10 October 2000.

Department of the Navy. "Analysis of Alternatives." *Navy Marine Corps Intranet (NMCI) Report to Congress* (n.p., Washington D.C. 30 June 2000).

Department of the Navy. "Executive Summary." *Navy Marine Corps Intranet (NMCI) Report to Congress* (Washington DC, 30 June 2000).

Department of the Navy Information Management & Information Technology (DON IM/IT) Pamphlet. *Catalog of DON IM/IT Strategic Goals, Tools, and Training* (n.p., July 2000).

Department of the Navy (Interim Guidance). "Information Management/Information Technology Inherently Governmental Functions" (n.p., 19 April 2000).

Deputy Assistant to the Secretary of the Navy for C4I/EW/Space. *Navy Marine Corps Intranet (NMCI) Execution.* 19 December 2000. 1.

Dobkins, James A.. "Federal Privatization and Outsourcing of Information Technology Functions: A Practitioner's Perspective." *Federal Contracts Report.* Vol. 66, No. 19, Nov 18, 1996.

Electronic Data Systems. "About EDS," URL: <http://www.eds.com/about_eds/en_about_eds.shtml>, viewed 7 January 2001.

Federal Computer Acquisition Center (FEDCAC). "Seat Management Overview" (12 July 2000). URL: http://fedcac.gsa.gov/seat.stm. accessed 7 September 2000.

Gabig, Jerome S. "Privatization: A Coming Wave for Federal Information Technology Requirements." *National Contract Management Journal.* Volume 27. Issue 1, 1996. quoting J. Collins and R. Millen. "Information systems Outsourcing by Large American firms: Choices and Impacts." *Information Resources Management Journal.* Winter, 1995.

General Services Administration (GSA) White Paper. "Outsourcing Information Technology" (February 1998) URL: <http://www.a76.com/refs/finalout.html>, accessed 7 September 2000.

Hayes, Heather. "Developing a Seat Management Strategy." *Federal Computer Weekly.* 24 August 1998. URL: http://208.201.97.5/ref/hottopics/seatmgmt/feat1.htm. accessed 17 September 2000.

Joint Chiefs of Staff. Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: GPO, 10 June 1998).

Joint Vision 2020. (Washington, DC: US Government Printing Office, June 2000).

Naval Sea Systems Command. Contract Number N00024-00-D-6000 (NMCI Contract).

Office of Management and Budget (OMB), Executive Office of the President. *Circular A-76 Supplement: Part I, Policy Implementation.* URL: <http://www.a76.com/refs/a076s1.html>. accessed 6 September 2000.

Office of Management and Budget, Executive Office of the President. Letter to the Honorable William S. Cohen, Secretary of Defense (Washington DC, September 12, 2000).

Ormerod, Gerald J. "Outsourced Logistics: Maximizing External Support." *Marine Corps Gazette.* Volume 81. Number 12. Quantico, Virginia. December 1997.

Rasmussen, David N. and Keith L. Ruegger. "A Functional Analysis of DOD Implementation of Seat Management." Naval Postgraduate School, Monterey, CA, September 1999.

Robinson, Bryan. "NASA JPL:A Seat Management Pioneer." *Federal Computer Weekly*, 24 August 1998. URL: http://208.201.97.5/ref/hottopics/seatmgmt/feat1.htm. accessed 17 September 2000.

Rosenburg, Rick. "*Executive Message: NMCI Well Under Way.* URL: http:<www.eds.com/nmci/exec_message_013101.htm>. viewed 17 February 2001.

Space and Naval Warfare Systems Command (SPAWAR) and NMCI Program Management Office (PMO). Department of the Navy. *Navy Marine Corps Intranet (NMCI) Execution Plan* (Washington DC, 13 September 2000).